Universidad de Cuenca

Facultad de Ingeniería

Maestría en Gestión Estratégica de Tecnologías de la Información

Proyecto de Tesis

METODOLOGÍA DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DEL RIESGO INFORMÁTICO APLICABLE A MPYMES

Autor:

Paúl Esteban Crespo Martínez, MBA

C.I. 0103559464

Director:

PhD. Francisco Rodrigo Salgado Arteaga

C.I. 0101493385

Resumen

La información es el elemento más valioso para cualquier organización o persona en este nuevo siglo, la cual, para muchas de ellas, es un arma para crear ventaja competitiva. Sin embargo, pese a la falta de conocimiento sobre cómo protegerla adecuadamente, o a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones, en especial el sector MPYME, no logra alcanzar este objetivo.

Por lo tanto, este estudio propone una metodología de seguridad de la información para la gestión del riesgo informático aplicable al entorno empresarial y organizacional del sector MPYME ecuatoriano. Para el efecto, se analizan comparativamente varias metodologías de amplia divulgación, como: Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III. Estas metodologías son internacionalmente utilizadas en la gestión del riesgo de información; a la luz de los marcos de referencia de la industria: ISO 27001, 27002, 27005 y 31000.

Palabras clave: riesgos, gestión, ECU@Risk, Seguridad de la Información.

Abstract

Information is the most valuable element for any organization or person in this new century, which, for many companies, is a competitive advantage asset. However, despite the lack of knowledge about how to protect it properly or the complexity of international standards that indicate procedures to achieve an adequate level of protection, many organizations, especially the MSMEs sector, fails to achieve this goal.

Therefore, this study proposes a methodology for information security risk management, which is applicable to the business and organizational environment of the Ecuadorian MSME sector. For this purpose, we analyze several methodologies as Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 COSO III. These methodologies are internationally used in risk management of information; in the light of the frameworks of the industry: ISO 27001, 27002, 27005 and 31000.

Keywords: Risk, Management, ECU@Risk, Information Security.

Tabla de contenido

Resumen 2
Abstract 3
Índice de ilustraciones 7
Índice de tablas 9
Cláusula de derechos de autor 10
Cláusula de propiedad intelectual 11
Agradecimientos 12
Introducción 13
Justificación del proyecto 15
Objetivo general 16
Objetivos específicos 16
Alcance del proyecto 16
Método de trabajo 17
Capítulo 1: Fundamentos 18
Las MPYMES 18
La seguridad de la información y el riesgo informático 21
El principio de defensa en profundidad 23
Los marcos de referencia internacionales utilizados en la gestión de riesgo 24
ISO/IEC 27001 25
ISO/IEC 27002:2005: 26
ISO/IEC 27005:2011 28
1. Establecimiento de plan de comunicación interno y externo. 28
2. Definición del contexto organizacional interno y externo. 29
3. Valoración de riesgos tecnológicos. 29
4. Tratamiento de riesgos tecnológicos. 30
5. Monitoreo y mejora continua del proceso de gestión. 30
ISO 31000:2009 30
Capítulo 2: Metodologías para la gestión de riesgos 32
Security Risk Management (Microsoft) 33
Magerit 35
CRAMM 36
Octave – S 38

Conclusiones del capítulo 2 41
Capítulo 3: Alineación de las metodologías con las normas ISO 45
Microsoft Risk Management 45
Octave – S 50
Magerit 52
CRAMM 54
Conclusiones del capítulo 56
Capítulo 4: Marco Legal 59
Delito Informático 59
Marco legal Internacional 62
Cuarta Enmienda 62
GLBA 63
HIPAA 64
Marco legal de la República del Ecuador 65
La Ley Orgánica de protección de datos personales. 65
Ley Orgánica de transparencia y acceso a la información pública 68
Ley de comercio electrónico 68
Junta Bancaria 69
Conclusiones del capítulo 4 71
Capítulo 5: Estado actual de las MPYMES en cuanto al riesgo de información 74
Conclusiones del capítulo 85
Capítulo 6: Proyección hacia COBIT 5 y COSO III 86
Introducción 86
COBIT 5 87
COSO III 90
Conclusiones del capítulo 6 91
Capítulo 7: Propuesta metodológica 94
Introducción 94
Parte A: Introducción al manejo del riesgo 94
Estándar de Gestión de Seguridad 95
Parte B: El marco de gestión de riesgo 100
Parte C: El proceso de gestión de riesgo 103
Paso 1: Determinación del contexto 104
Paso 2: Identificar los activos de información 116

Paso 3: Identificación de los riesgos 129
[NATURALES] Errores y fallos no intencionados 131
[PROVOCADO] Errores y fallos no intencionados 132
[NO_INTENCIONADO] Errores y fallos no intencionados 132
Paso 4: Análisis de los riesgos 135
Paso 5: Evaluación de los riesgos 137
Paso 6: Tratamiento de los riesgos 139
Paso 7: Identificación de contramedidas 143
Paso 8: Monitoreo y revisión 147
Paso 9: Comunicar y consultar 149
Parte D: Recursos 150
Matriz para la identificación de activos de información 150
Hardware 150
Software 150
Información Electrónica 150
Información Electrónica 150
Infraestructura de comunicaciones 151
Medios de almacenamiento extraíbles 151
Recursos humanos 151
Edificaciones / Instalaciones 151
Matriz para el registro de riesgos 152
Registro y cálculo de riesgos 152
Matriz para el manejo de riesgos 152
Cuestionario sobre aplicabilidad de la metodología 153
Aspectos considerados en la construcción de ECU@Risk 157
Conclusiones 160
Glosario 173
Bibliografía y fuentes de consulta. 175
Referencias 176

Índice de ilustraciones

Ilustración 1: Principio de defensa en profundidad. Fuente: (Gómez Vieites, 2011) 24
Ilustración 2: Principio de defensa en profundidad. Fuente: (Vásquez & López, 2016) Elaborado por: El autor 35
Ilustración 3: Actividades económicas según el INEC 2015. Fuente: INEC, 2015 77
Ilustración 4: Actividad a la que se dedican las empresas estudiadas. Desarrollado por: El Autor 79
Ilustración 5: Identificación de los activos de información. Fuente: Estudio realizado por el Autor 80
Ilustración 6: Actualización del inventario de activos de información. Fuente: Estudio realizado por el autor 80
Ilustración 7: Realiza respaldos. Fuente: Estudio realizado por el autor 81
Ilustración 8: Realiza respaldos bajo procedimientos formales. Fuente: Estudio realizado por el autor. 82
Ilustración 9: Delimitación formal de las áreas físicas sensibles. Fuente: Estudio realizado por el autor 82
Ilustración 10: Procedimientos para evacuación de edificios. Fuente: Estudio realizado por el autor. 83
Ilustración 11: Amenazas identificadas de manera formal. Fuente: Estudio realizado por el autor. 84
Ilustración 12: Planes formales para la gestión de riesgo de información. Fuente: Estudio realizado por el autor. 84
Ilustración 13: Razones por las que las empresas no han adoptado un plan de gestión de riesgos formal. Fuente: Estudio realizado por el autor. 85
Ilustración 14: Elementos de la gestión de riesgo. Fuente: (University of Adelaide, 2015). Desarrollado por: El Autor 97
Ilustración 15: El proceso de gestión de riesgo basado en el modelo de Deming. Elaborado por: El autor 103
Ilustración 16: Clasificación de los activos de información 116
Ilustración 17: Criterios de valoración. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 128
Ilustración 18: Clasificación de los riesgos de información organizacionales. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012). Desarrollo: Autoría propia. 131
Ilustración 19: Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 132
Ilustración 20: Errores de los usuarios. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 132
Ilustración 21: Errores del administrador. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 133
Ilustración 22: Errores de monitorización. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 133
Ilustración 23: Errores de configuración. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 133

Ilustración 24: Deficiencias de la organización. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 134
Ilustración 25: Alteración accidental de la información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 134
Ilustración 26: Destrucción de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 134
Ilustración 27. Difusión de software dañino. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 134
Ilustración 28. Copia no controlada de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 135
Ilustración 29: Escapes de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 135
Ilustración 30: Errores de re-encaminamiento. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 135
Ilustración 31: Errores de secuencia. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 135
Ilustración 32: Matriz de Riesgo. Fuente: (University of Adelaide, 2015) 137
Ilustración 33: Acción de gestión requerida. Fuente (University of Adelaide, 2015) 139
Ilustración 34: Tipos de protección. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 144
Ilustración 35: Matriz de inventario de activos de hardware. Fuente: Autoría propia 150
Ilustración 36: Matriz de inventario de activos de software. Fuente: Autoría propia 150
Ilustración 37: Matriz de inventario de activos de Información electrónica. Fuente: Autoría propia 150
Ilustración 38: Matriz de inventario de activos de Información en papel. Fuente: Autoría propia 150
Ilustración 39: Matriz de inventario de activos de Infraestructura de comunicaciones. Fuente: Autoría propia 151
Ilustración 40: Matriz de inventario de activos de Medios de almacenamiento extraíbles. Fuente: Autoría propia 151
Ilustración 41: Matriz de inventario de activos Recursos Humanos. Fuente: Autoría propia 151
Ilustración 42: Matriz de inventario de activos de Edificaciones / Instalaciones. Fuente: Autoría propia 151
Ilustración 43: Matriz para el registro de riesgos. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012) 152
Ilustración 44: Registro y cálculo de riesgos. Fuente: (27001 Academy, 2015) 152
Ilustración 45: Matriz de Riesgo. Fuente: (University of Adelaide, 2015) 152
Ilustración 46: Acción de gestión requerida. Fuente (University of Adelaide, 2015) 153
Ilustración 47: Cuestionario sobre aplicabilidad de la metodología. Fuente:ISO 27001 ... 156

Índice de tablas

Tabla 1: Participación de las empresas del sector MPYME en el Ecuador. Fuente: (Universidad Andina Simón Bolivar, 2011), Elaborado por: El autor. 19
Tabla 2: Clasificación de las MPYMES de acuerdo al volumen de ventas. Fuente: (Universidad Andina Simón Bolivar, 2011) Elaborado por: El autor. 20
Tabla 3: Clasificación de las MPYMES por el número de personas ocupadas. Fuente: (Universidad Andina Simón Bolivar, 2011) Elaborado por: El autor 20
Tabla 4: Vulnerabilidades y frecuencias *Fuente: (Castaño, 2014)* 22
Tabla 5: Proceso para la gestión de riesgos ISO 27005. Fuente: (Vásquez & López, 2016), (Moncayo Racines, 2014) 28
Tabla 6: Metodologías utilizadas para la gestión de riesgo informático. Fuente: (Vásquez & López, 2016) 33
Tabla 7: Distribución de las empresas a evaluar. 78
Tabla 8: Clasificación de las sociedades. Fuente: SRI. Elaborado por: El autor 106
Tabla 9: Clasificación de la organización por su tamaño. Fuente: (Vásquez & López, 2016) (Muñoz, 2012). Elaborado por: El autor 106
Tabla 10: Cuadro de análisis PESTEL. Fuente: (Azanza & Bermeo, 2016) 111
Tabla 11: Matriz para identificación del FODA institucional. Fuente: (Azanza & Bermeo, 2016) 111
Tabla 12: Matriz para identificación de roles y actividades incompatibles. Fuente: Autoría Propia 113
Tabla 13: Matriz para la identificación de habilidades. Fuente: Autoría propia 113
Tabla 14: Matriz para la identificación de Valores compartidos organizacionales. Fuente: Autoría propia 114
Tabla 15: Matriz de identificación del estilo organizacional. Fuente: Autoría Propia 115
Tabla 16: Matriz de identificación del estilo organizacional. Fuente: Autoría propia 115

Cláusula de derechos de autor

Universidad de Cuenca
Clausula de derechos de autor

Paúl Esteban Crespo Martínez, autor/a de la tesis "Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Magister en Gestión Estratégica de Tecnologías de Información. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor/a

Cuenca, 29 de noviembre de 2016

Paúl Esteban Crespo Martínez

C.I: 0103559464

Cláusula de propiedad intelectual

Universidad de Cuenca
Clausula de propiedad intelectual

Paúl Esteban Crespo Martínez, autor/a de la tesis "Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 29 de noviembre de 2016

Paúl Esteban Crespo Martínez

C.I: 0103559464

Agradecimientos

Agradezco a mi Director, Dr. Francisco Salgado Arteaga, por el tiempo brindado en la dedicación y apoyo a este proyecto…

…A mis alumnos Geovanna, Pablo, Santiago, David, y Belén, por el fuerte esfuerzo en la dedicación y contribución intelectual…

… Y de manera muy especial a mi esposa Susana, a mis hijos Josué y Nicolás; a mis padres, Miguel y María, a mi hermana Verónica, y a mis sobrinos Daniela, Estefanía y Mateo… gracias por su paciencia y apoyo incondicional durante todo este tiempo…

Introducción

La Seguridad de la Información se basa en tres principios fundamentales: La integridad que hace referencia a que la información debe estar libre de alteraciones o modificaciones no planificadas, la disponibilidad que indica que la información debe ser utilizable cuando se la requiera, y confidencial porque solo debe ser accedida por los que lo requieren. La mala administración, o la carencia de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización, puede conllevar a un efecto llamado Riesgo Operativo.

El Riesgo Operativo consiste en la posibilidad de que se produzcan pérdidas debido a los eventos originados, ya sea por fallas en procesos, personas, sistemas internos, tecnología, o por eventos externos imprevistos; lo que indica que el acceso a la información deberá ser correctamente controlado, otorgando los permisos a quienes tengan autorización de los propietarios de la información. Para ello es necesaria una adecuada gestión de los perfiles de usuario y acceso a la misma.

El objetivo de este proyecto de grado es el de proponer una metodología para la Gestión del Riesgo Informático que permita aplicarse al entorno ecuatoriano, a fin de identificar y registrar sus activos de información, comprendiendo que estos son: Hardware, Software, Información electrónica y bases de datos, procedimientos de gestión de usuarios, Sistemas de comunicaciones, servicio provisto por terceros y elementos de respaldo; para luego identificar y valorar los riesgos y amenazas, tanto físicas o de entorno, como lógicas; permitiendo finalmente desarrollar un adecuado Sistema de Gestión de Seguridad de la Información, en base a estudios comparativos de las metodologías Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III, utilizadas en la gestión del riesgo de información y el riesgo informático; aclarando que las mismas están alineadas a los requerimientos de las normas internacionales ISO 27001, 27002, 27005 y 31000.

Las MPYMES ecuatorianas están inmersas en un eminente entorno de riesgo, ya sea a nivel nacional por la inestabilidad política y/o económica; o regional debido a las condiciones naturales en las que se asienta cada ciudad. Además, consideran que la informática es

solamente un área de soporte, y que la inversión en elementos y mecanismos de seguridad convergen solamente en una solución antivirus. El desconocimiento, la exigencia y extensión de las normas, ayudan a que el concepto de gestión de riesgo informático quede como un mito empresarial.

El presente trabajo tiene diversas aristas que lo hacen atractivo desde los diferentes puntos de vista con los que se lo pueda evaluar, involucrando varias acciones relacionadas con el quehacer académico universitario y la concordancia con la normativa existente:

- La articulación de la Investigación Institucional con el Plan Nacional de Desarrollo.
- El Plan Nacional del Buen Vivir y sus lineamientos estratégicos
- Ley Orgánica del Sistema Nacional de Gestión de Riesgos

Finalmente, se puede decir que este trabajo sería considerado como un importante eje transversal para asegurar la información que acompaña a muchos procesos productivos de las MPYMES nacionales, permitiendo a las empresas de este sector mantener la información disponible, integra y confidencial, dentro de un marco de riesgo analizado.

Justificación del proyecto

De la indagación exploratoria realizada, no se encuentra alguna organización, institución o empresa ecuatoriana que haya emprendido en la tarea del desarrollo de una metodología para la gestión del Riesgo de Información que considere la realidad nacional en el entorno MPYME. Las Instituciones de control se han limitado a solicitar la implementación de prácticas internacionales, que muchas veces ni las grandes empresas logran cumplir, debido a la cantidad de parámetros y procedimientos exigidos por las normas.

Este proyecto se inserta en el proyecto de investigación "Propuesta metodológica para la gestión del riesgo informático en PYMES", que el autor de esta propuesta dirige en la Escuela de Sistemas y Telemática de la Universidad del Azuay. Por su naturaleza multidisciplinar, el proyecto vincula los ámbitos académicos de la administración y los de ingeniería relacionadas con Tecnologías de Información, además de permitir la vinculación con la sociedad en general y con el aparato productivo en particular.

Objetivo general

Desarrollar una metodología de seguridad de la información para la gestión del riesgo informático de las organizaciones del sector MPYME, aplicable al entorno ecuatoriano.

Objetivos específicos

- Realizar un análisis comparativo entre tres metodologías internacionales utilizadas en el análisis y gestión de riesgo informático, en base a mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo.
- Estudiar los aspectos de regulación local, nacional e internacional y normas que tratan el riesgo
- Desarrollar una metodología para el análisis y gestión de riesgo informático en las empresas del sector MPYME.

Alcance del proyecto

El alcance de este proyecto de tesis es realizar un cuadro comparativo de las metodologías Magerit, CRAMM, Octave y Microsoft RISK para la gestión de riesgo; su alineación con los marcos de referencia ISO 27001, 27002, 27005 y 31000; para luego proponer una metodología que sea adaptable al entorno MPYME ecuatoriano, considerando su proyección a COBIT 5 y COSO III.

Método de trabajo

Esta tesis contempla ser desarrollada metodológicamente en dos etapas generales.

Etapa 1: Análisis comparativo de metodologías internacionales

En esta primera etapa, de todos los elementos mencionados, se hará hincapié en el estudio de las normativas internacionales ISO utilizadas en la gestión de riesgo informático, el comparativo de tres metodologías para la gestión de riesgo informático, y el estudio de los marcos de gobierno de TI y gestión de riesgo COBIT y COSO. El levantamiento de la línea base de la investigación contará con la colaboración de los estudiantes de carreras de grado que realizan sus trabajos de titulación en el marco del proyecto de la Universidad del Azuay señalado.

Etapa 2: Propuesta

Caracterizar las PYMES de la región austral del Ecuador en relación con las TI y la seguridad de la información, en base a lo cual se desarrollará y propondrá una metodología para la gestión de riesgo informático, con referentes nacionales, aplicable al entorno ecuatoriano.

Capítulo 1: Fundamentos

Las MPYMES

Partiendo de lo conceptual, el término MPYME hace referencia a las micro, pequeñas y medianas empresas, concepto que según (Vásquez & López, 2016), citando a (Muñoz, 2012), en el Ecuador está clasificado de la siguiente manera:

Microempresa: Este tipo de empresa está comprendida de escasos ingresos y está compuesta de 1 a 10 empleados involucrados exclusivamente. Las microempresas tienen los siguientes criterios:

- El número de empleados es igual o menor a 10 personas.
- El volumen anual de negocio no supera los 20 mil dólares.

Este tipo de empresa tiene la ventaja de ser flexibles, es decir que pueden adaptarse fácilmente a los cambios del mercado. (Muñoz, 2012) (Vásquez & López, 2016)

Pequeña empresa: Es una entidad independiente, creada para generar rentabilidad, su ritmo de crecimiento es superior al de la microempresa y puede ser mayor al de la mediana o grande y cumplen con los siguientes criterios:

- El número de empleados es mayor a 50 personas.
- El volumen anual de negocio supera los 20 mil dólares.

(Muñoz, 2012) (Vásquez & López, 2016)

Mediana Empresa: Las medianas empresas se caracterizan a que el capital es suministrado por sus propietarios, su tamaño es relativamente pequeño dentro del sector en el que se desarrolla, estas empresas aseguran el mercado de trabajo mediante la descentralización de obra.

- Alberga entre 50 a 99 empleados
- Su capital fijo no debe sobrepasar los 120 mil dólares.

(Muñoz, 2012) (Vásquez & López, 2016)

Según un informe del Observatorio PYME de la Universidad Andina Simón Bolivar, en Ecuador, las 10 actividades económicas principales de este segmento empresarial, de acuerdo a su participación en el mercado, son:

Actividad económica	Participación
Venta al por menor en comercios no especializados con predominio de la venta de alimentos, bebidas y tabaco	17,4%
Actividades de restaurantes y de servicio móvil de comidas	8,9%
Venta al por menor de prendas de vestir, calzado y artículos	5,1%
Mantenimiento y reparación de vehículos automotores	4,1%
Otras actividades de telecomunicaciones	3,5%
Venta al por menor de alimentos, bebidas y tabaco en puestos	3,1%
Otras actividades de venta al por menor en comercios no especializado	3,1%
Venta al por menor de alimentos en comercios especializados	2,9%
Actividades de peluquería y otros tratamientos de belleza.	2,9%
Venta al por menor de productos farmacéuticos y medicinales	2,2%
Los 229 sectores restantes	46,7%

Tabla 1: Participación de las empresas del sector MPYME en el Ecuador. Fuente: (Universidad Andina Simón Bolivar, 2011), Elaborado por: El autor.

De acuerdo al volumen de ventas, las MPYMES también pueden clasificarse de la siguiente manera:

Actividad económica	Participación
Fabricación de productos de la refinación del petróleo.	5,7%
Fabricación de otros productos elaborados de metal n.c.p.	5,0%
Venta al por mayor de combustibles sólidos, líquidos y gaseosas	4,9%
Venta de vehículos automotores.	4,4%
Venta al por mayor de alimentos, bebidas y tabaco.	4,0%

Venta al por mayor de otros enseres domésticos.	3,1%
Otros tipos de intermediación monetaria	2,9%
Fabricación de productos farmacéuticos, sustancias químicas.	2,6%
Venta al por menor en comercios no especializados con predominio de la venta de alimentos, bebidas y tabaco	2,5%
Fabricación de otros hilos y cables eléctricos.	2,5%
Los 229 sectores restantes	62,3%

Tabla 2: Clasificación de las MPYMES de acuerdo al volumen de ventas. Fuente: (Universidad Andina Simón Bolivar, 2011) Elaborado por: El autor.

Así mismo, sugiere clasificarlas por el número de personas ocupadas. De esta manera, las 10 actividades económicas principales del país se resumen en la siguiente tabla:

Actividad económica	Participación
Venta al por menor en comercios no especializados con predominio de la venta de alimentos, bebidas y tabaco	7,1%
Actividades de restaurantes y de servicio móvil de comidas.	5,9%
Enseñanza preprimaria y primaria.	4,7%
Enseñanza secundaria de formación general.	3,7%
Actividades de la administración pública en general.	3,4%
Venta al por menor de prendas de vestir, calzado y artículos	2,4%
Mantenimiento y reparación de vehículos automotores	2,4%
Actividades de mantenimiento del orden público y de seguridad	2,3%
Actividades de médicos y odontólogos	2,0%
Actividades de hospitales y clínicas	2,0%
Los 229 sectores restantes	64,2%

Tabla 3: Clasificación de las MPYMES por el número de personas ocupadas. Fuente: (Universidad Andina Simón Bolivar, 2011) Elaborado por: El autor

Para Marcela Pérez, las operaciones en una MPYME cobran día a día más importancia, debido al inusual crecimiento de tres factores externos: competencia, globalización y nuevas tecnologías; en el que la participación de los clientes agrega el componente esencial que motiva a las empresas y organizaciones a estar alerta y preparada, conocida como el

valor agregado. Así, las empresas y organizaciones deben responder rápidamente a las situaciones de entorno, siendo las decisiones operacionales de carácter táctico y estratégico, en las que el insumo fundamental es la información (Pérez, 2011).

La seguridad de la información y el riesgo informático

Existen múltiples definiciones para la seguridad de la información. Una de ellas es: "la protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo" (Royer, 2004)

Para Germán Alcides, el riesgo informático es un conjunto de normas y procedimientos que son aplicados para salvaguardar un sistema informático, cuya finalidad es garantizar que todos los recursos que conforman el sistema informático sean utilizados para el fin que fueron creados sin ninguna intromisión (Alcides, 2009).

De las definiciones anteriores se desprende que la seguridad de la información se fundamenta en tres principios básicos: confidencialidad, disponibilidad e integridad; entendiéndose por confidencialidad a los mecanismos que garantizan el acceso a la información a personas y organismos autorizados, por integridad a la consistencia de la información almacenada, y por disponibilidad a la característica de que la información debe estar disponible en el momento que sea requerida.

La seguridad de la información contempla como actores a los elementos que de una u otra forma están involucrados con el manejo de la información, tanto digital como física dentro de una organización. Así, por ejemplo, la metodología Magerit contempla al hardware, software, información electrónica, recurso humano, entre otros, como actores que consumen y producen información.

La información, para cualquier organización, ya sea pública o privada, tiene valor monetario. Por ejemplo, para el Servicio de Rentas Internas, la base de datos de sus contribuyentes es esencial, o la base de datos de los sujetos de crédito para un banco son

muy importantes. Las instituciones, organismos y empresas deben preguntarse: ¿Cuánto vale esa información para mi organización, y cuánto para mi competencia? La información esencial puede ser un objetivo muy atractivo para un tercero, y muchas veces, por descuido o por desconocimiento, la misma puede verse comprometida.

La vulnerabilidad hace referencia a las debilidades que existen en un sistema de información, lo que permite que pueda ser fácilmente atacado, evadiendo el control de acceso y la confidencialidad de los datos y las aplicaciones existentes (Cordero Torres, 2015). Las vulnerabilidades deben ser expresadas en una escala numérica para poder posteriormente cuantificar su impacto, y, citando a Burgos y Campos, se sugiere que éstas sean identificadas y valoradas individualmente (Cordero Torres, 2015) (Burgos Salazar & Campos, 2008)
La vulnerabilidad, de acuerdo a Pablo Castaño, debe ser expresada mediante la fórmula básica:

Vulnerabilidad=Frecuencia estimada / Días al año (Cordero Torres, 2015) (Castaño, 2014)
Esto significa que la vulnerabilidad se da por el número de ocurrencias que puedan presentarse en un tiempo. Así Castaño sugiere la siguiente escala de frecuencias de repetición y el tipo de vulnerabilidad presentada.

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada dos semanas	26/365 = 0.071
Frecuencia media	1 vez cada dos meses	0.016
Frecuencia baja	1 vez cada 6 meses	0.005
Frecuencia muy baja	1 vez al año	0.002

Tabla 4: Vulnerabilidades y frecuencias *Fuente: (Castaño, 2014)*

Las amenazas son los elementos que pueden dañar o alterar la información de una u otra forma. Estas generalmente pueden ser encontradas a partir de una vulnerabilidad existente. El riesgo a su vez, es la probabilidad que tiene una amenaza para originarse y que puede generar un cierto impacto en la organización.

El principio de defensa en profundidad

El principio de defensa en Profundidad es un modelo en capas que sugiere establecer varios niveles de seguridad dentro del sistema de seguridad informático que mantiene una organización, los mismos que permitan mitigar o retrasar un ataque. (Gómez Vieites, 2011) (Vásquez & López, 2016)

El dejar abandonado un sistema luego de su implementación no garantiza la seguridad. Por lo tanto, en los sistemas informáticos se deberá contar con un control y monitoreo constante, el mismo que será realizado mediante la configuración a conciencia de servidores y equipos informáticos, analizando e instalando sus debidas actualizaciones y eliminando todo tipo de vulnerabilidades. Además, los administradores de infraestructura deberán, por seguridad, desactivar o inhabilitar los servicios que son innecesarios, considerando además con un permanente cambio de contraseñas, aplicando el concepto de rotación y el uso de claves seguras. Según Vásquez y López, citando a Álvaro Gómez, se puede comprobar que, con este modelo, los atacantes solo se atreverán a lidiar con sistemas informáticos débiles. (Gómez Vieites, 2011) (Vásquez & López, 2016)

Para Gómez, el principio de defensa en profundidad se resume como:

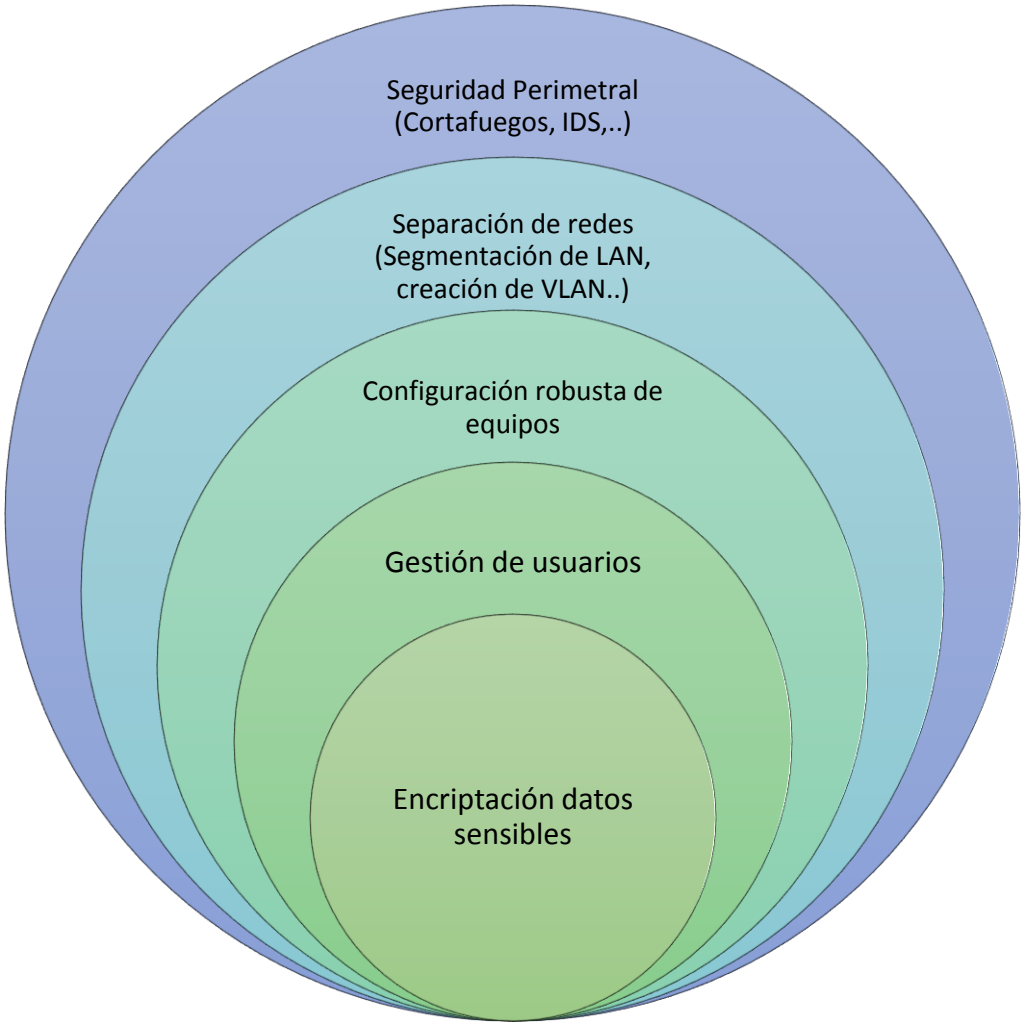


Ilustración 1: Principio de defensa en profundidad. Fuente: (Gómez Vieites, 2011)

Es por esa razón que no se puede confiar en la seguridad brindada en una única capa, sino que el éxito se logra cuando se va reforzando cada una de las mismas, a manera de lograr un adecuado mix de tecnologías, técnicas y estrategias.

Los marcos de referencia internacionales utilizados en la gestión de riesgo

Con el objetivo de estandarizar los procesos y actividades para la gestión de riesgo, la Organización Internacional para Estandarización (ISO) agrupa a las mejores prácticas de la industria en la familia ISO 27000, a manera de aconsejar a las organizaciones en el desarrollo, implementación y administración de un sistema de gestión de seguridad de la

información o SGSI. A continuación, se detallan los estándares que pertenecen a la familia ISO 27000.

ISO/IEC 27001

Publicada el 15 de octubre de 2005, y basada en el modelo de Deming, proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de seguridad de la información. El marco referencial es aplicable a todo tipo de organización, pues es bastante extensa en cuanto a su aplicación y controles operacionales.

Para Cordero, la ISO 27001 está constituida por los siguientes dominios:

- **La política de seguridad,** cuyo objetivo es garantizar el soporte y gestión necesarios para la seguridad, según los requisitos institucionales y normativos.
- **La organización de la seguridad de la información,** cuya finalidad es instaurar un marco de referencia para la implementación y control de la seguridad de la información.
- **La gestión de activos,** que tiene como objetivo asegurar los activos de la organización.
- **La seguridad de los recursos humanos,** cuyo objetivo es fijar las medidas necesarias para controlar la seguridad de la información, que sea manejada por los recursos humanos.
- **La seguridad física y del ambiente,** que busca proteger a las instalaciones de la organización y a toda la información que maneja.
- **La gestión de las comunicaciones y operaciones,** que permite determinar el procedimiento y responsabilidades de las operaciones que realiza la organización.
- **El control de acceso,** con el que se asegura la confidencialidad de los sistemas de información de la organización.
- **La adquisición, desarrollo y mantenimiento de los sistemas de información,** dirigida a organizaciones que desarrollen software internamente o que tengan un contrato con otra organización que sea la encargada de desarrollarlo.

- **La gestión de incidentes en la seguridad de la información,** que aplica un proceso de mejora constante en la gestión de percances de seguridad de la información.
- **La gestión de la continuidad del negocio,** cuyo objetivo es garantizar la continuidad operativa de la organización.
- **El cumplimiento,** que busca asegurar que los requisitos legales de seguridad, referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan (Cordero Torres, 2015).

ISO/IEC 27002:2005:

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información. Es una norma que permite crear principios para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información, posee objetivos de control se implementan para satisfacer los requisitos analizados por la evaluación de riesgos. (Cordero, 2015), (Vásquez & López, 2016).

Según Crespo y Cordero, 2016, ISO 27002 establece directrices y principios generales para la iniciación, implementación, mantenimiento y mejora de la gestión de seguridad de la información en una organización. Está estructurada en 16 capítulos (27001 Academy, 2015), los mismos que se citan a continuación:

- **Conceptos generales:** Fundamentos de seguridad de la información y SGSI.
- **Campo de aplicación:** capítulo que especifica el objetivo de la norma y su campo de aplicación.
- **Términos y definiciones:** contiene una breve descripción de los términos más usados en la norma.
- **Estructura del estándar:** describe la estructura de la norma.
- **La evaluación y tratamiento del riesgo:** incluye procedimientos y detalles sobre evaluación y tratamiento de los riesgos de seguridad de la información.
- **La política de seguridad:** presenta los mecanismos para establecer controles que

permitan orientar a la alta dirección sobre la seguridad de la información.

- **La gestión de activos:** da las pautas para establecer controles que permitan lograr y mantener la protección adecuada de los activos de información de la organización.
- **Seguridad ligada a los recursos humanos:** recomienda controles para el aseguramiento de los empleados, contratistas y usuarios de terceras partes.
- **Seguridad física y ambiental:** proporciona controles que permitan evitar el acceso físico no autorizado, el daño o la interferencia en las instalaciones y a la información de la organización, de igual forma evitar la pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.
- **La gestión de comunicaciones y operaciones:** orientada al establecimiento de controles que permitan asegurar la operación correcta y segura de los servicios de procesamiento de información e implementar y mantener un grado adecuado de seguridad de la información, de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros.
- **El control de acceso:** con prácticas que permitan controlar el acceso a la información de la organización con base en los requisitos de seguridad y del negocio, y asegurar la confidencialidad de los sistemas de información.
- **La adquisición, desarrollo y mantenimiento de los sistemas de información:** su objetivo es proporcionar lineamientos que garanticen la seguridad en los procesos de adquisición, mantenimiento y desarrollo del software.
- **La gestión de incidentes de seguridad de la información:** propone controles que permitan asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información, y la forma de comunicar.
- **La gestión de la continuidad del negocio:** propone controles orientados a contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra fallos y desastres.
- **El cumplimiento:** donde se establecen controles de cumplimiento legal, obligaciones estatuarias reglamentarias o contractuales y de cualquier requisito de seguridad (Cordero Torres, 2015), (Crespo & Cordero, 2016)

ISO/IEC 27005:2011

Esta norma es compatible con los conceptos generales especificados en la norma ISO/IEC 27001; contiene la descripción de los procesos para la gestión del riesgo en la seguridad de la información y sus actividades y proporciona directrices para gestión de riesgos. Está pensada para ser aplicada en todo tipo de organizaciones que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización (Cordero Torres, 2015).

La gráfica a continuación permite visualizar los procesos que forman parte de la norma ISO 27005.

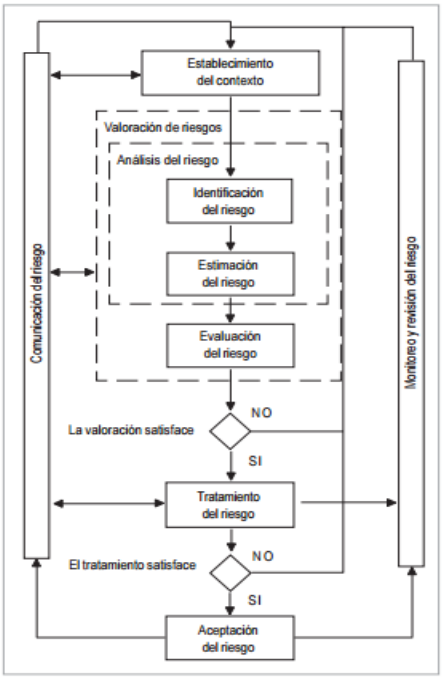


Tabla 5: Proceso para la gestión de riesgos ISO 27005. Fuente: (Vásquez & López, 2016), (Moncayo Racines, 2014)

Las cinco etapas que comprende la ISO 27005 según (Vásquez & López, 2016) y (Crespo & Cordero, 2016), son las siguientes:

1. Establecimiento de plan de comunicación interno y externo.

Esta planificación es realizada a nivel interno (empleados, directivos, socios) y externo (distribuidores, clientes), a través de charlas informativas, presentaciones, circulares,

capacitaciones. El objetivo es crear conciencia en seguridad, y evidenciar la existencia de riesgos tecnológicos.

Contiene tres etapas:

1. **Comunicación inicial:**

Aquí se conceptualiza el riesgo y sus implicaciones, las ventajas de la gestión, entre otros.

2. **Comunicación sobre la marcha.**

Consiste en presentar a cada uno de los miembros de la organización los resultados obtenidos durante el proceso de establecimiento de un plan de mitigación de riesgos, con el fin de retroalimentar el proceso.

3. **Comunicación de resultados.**

Comunica los resultados considerando la confidencialidad de la misma, es decir que la información no será de conocimiento público.

2. Definición del contexto organizacional interno y externo.

Es obligatorio e imprescindible conocer el entorno organizacional, con el objetivo de determinar las afecciones que podrían presentarse tanto a nivel interno como externo, además de evaluar y estipular lo que se requiere proteger, y los mecanismos para realizar esta actividad.

3. Valoración de riesgos tecnológicos.

En esta etapa lo que se recomienda es identificar los activos de información que se protegerán, así como sus debilidades y amenazas.

Para una correcta valoración se debe priorizar los activos incluyendo procesos, información, datos y activos de soporte.

Sin olvidar de que se debe identificar los tipos de amenazas, los daños que implican cada una de estas amenazas, perdidas que causan los riesgos en términos de impacto y un análisis sobre el negocia más conocido como BIA (*Bussines Impact Analysis).*

4. Tratamiento de riesgos tecnológicos.

En esta etapa lo que se implementan las acciones (reducir, aceptar, eliminar, transferir) a tomar para mitigar los riesgos anteriormente analizados.

Estas acciones junto con un plan de tratamiento en donde se definen recursos, responsabilidades se debe documentar para finalmente definir las políticas a seguir.

5. Monitoreo y mejora continua del proceso de gestión.

En esta fase el elemento necesario es el control de cambios, el monitoreo se realiza sobre los activos identificados, vulnerabilidades, procesos, amenazas, documentación, políticas y procedimientos con el fin de establecer acciones ante algún cambio.

Lo que se busca con el monitoreo es mantener a los riesgos controlados y ante la posibilidad de que aparezcan después nuevos riesgos poderlos controlar antes de que realicen algún daño a los activos de información.

(Ramírez y Ortiz, 2011)

ISO 31000:2009

Publicada en noviembre del 2009, y como resultado del estándar de riesgo de Nueva Zelanda/Australia (AS NZS 4360:2004), esta norma hace referencia a los principios y directrices, marco y procesos para la gestión de riesgos., el mismo que puede ser adoptado por cualquier organización (Cordero Torres, 2015) (Vásquez & López, 2016).

La norma recomienda las mejores prácticas a las organizaciones para que puedan establecer un marco de trabajo (framework), considerando cada una de las etapas de gestión: Planificación, desarrollo, despliegue, monitoreo y mejora continua.

Con el objetivo de lograr mayor eficacia con ISO 31000, Vásquez y López argumentan que se debe considerar los siguientes principios para una adecuada gestión de riesgos:

a) Crea valor.
b) Está integrada a los procesos de organización.
c) Forma parte de la toma de decisiones.

d) Trata explícitamente la incertidumbre.
e) Es sistemática, estructurada y adecuada.
f) Hecha a la medida.
g) Hace énfasis en los factores humanos y culturales.
h) Basada en la mejor información disponible.
i) Es transparente e inclusiva.
j) Dinámica, iterativa y sensible al cambio.
k) Facilita la mejora continua de la organización.

La ISO 31000 mejora la gobernabilidad en las organizaciones, ya que enfoca a la dirección en lograr una adecuada eficacia y eficiencia laboral, mediante la identificación de amenazas y oportunidades, la minimización de pérdidas, en la implementación y uso adecuado de controles, y además en mejorar la capacidad de recuperación ante eventos de desastre (Vásquez & López, 2016).

Capítulo 2: Metodologías para la gestión de riesgos

Una metodología es una de parte de la lógica que estudia los métodos. Según el diccionario de la Real Academia Española, la palabra metodología hace referencia al *"conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal"*; por consiguiente, puede entenderse como el conjunto de procedimientos que determinan una investigación, ya sea científica o una exposición doctrinal. Enfocándose en el riesgo informático y el riesgo de tratamiento de la información, el presente capítulo pretende evaluar las metodologías Magerit, CRAMM, Risk, y Octave-S, las mismas que posteriormente serán analizadas, validando su alineación con las normativas que sugieren las mejores prácticas para la gestión de riesgos.

Existen diversas metodologías para la gestión de riesgos. Según (Vásquez & López, 2016), entre las más conocidas están:

Metodología	**Descripción**	**Organización**	**Origen**
CMMI	*Capability Maturity Model Integration.*	*SEI (Software Engineering Institute).*	Estados Unidos
SPICE	*Software Process Improvement and Capability Determination.*	*ISO (International Organization for Standardization)*	International (Suiza)
PMBOK	*Project Management Body of Knowledge*	*PMI (Project Management Institute)*	Estados Unidos.
COBIT	*Control Objectives for Information and related Technology*	*ISACA (Information Systems Audit and Control Association)*	Estados Unidos.
OCTAVE	*Operationally Critical Threat Asset and Vulnerability Evaluation.*	*Carnegie Mellon SEI (Software Engineering Institute) y CERT (Computer Emergency Response Team)*	Estados Unidos.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT.	MAP (Ministerio de Administraciones Públicas)	España

SECURITY RISK MANAGMENT GUIDE	Administración de Riesgos de Seguridad.	Microsoft.	Estados Unidos.
CRAMM	CCTA Risk Analysis and Management Method	Agencia Central de Cómputo y Telecomunicaciones - CCTA	Reino Unido

Tabla 6: Metodologías utilizadas para la gestión de riesgo informático. Fuente: (Vásquez & López, 2016)

Security Risk Management (Microsoft)

Security Risk Management es una metodología para la gestión de riesgos desarrollada por Microsoft en el 2006. (Vásquez & López, 2016) citando a Microsoft, mencionan que el objetivo de Secure Risk Management es *"ofrecer una orientación clara sobre cómo implementar un proceso de gestión de riesgos de seguridad que ofrece una serie de beneficios, incluyendo:*

- *Mover los clientes a una postura de seguridad proactiva y liberándolos de un proceso reactivo, frustrante.*
- *Realización de seguridad medible mostrando el valor de los proyectos de seguridad.*
- *Ayudar a los clientes a mitigar eficazmente los riesgos más grandes en sus entornos en lugar de aplicar los recursos escasos para todos los riesgos posibles."*

Esta guía metodológica ofrece a las organizaciones una perspectiva clara y de fácil comprensión para organizar y asignar prioridades a cada recurso (activo de información), con el objetivo de identificar y gestionar adecuadamente los riesgos que pueden o suelen presentarse. Además, esta guía puede crear ventajas, las cuales se aprecian únicamente al implementar correctamente los controles propuestos, ya que ayudan a reducir el riesgo a un nivel aceptable. (Microsoft, 2006).

La clave de la guía de Microsoft está en el enfoque general que mantiene la guía. Según la investigación realizada por (Vásquez & López, 2016), *"Cada capítulo se basa en una práctica completa necesaria para iniciar y poner en funcionamiento de forma eficaz un*

proceso de administración de riesgos de seguridad continuo en la organización" (Microsoft, 2006), (Vásquez & López, 2016).

Así, la guía está clasificada en los siguientes capítulos:

1. Introducción a la guía de administración de riesgos de seguridad, en el que se ofrece una vista panorámica a la metodología.
2. Estudio de prácticas de administración de riesgos de seguridad, en el que se realiza el análisis de puntos débiles y fuertes de cada uno de los enfoques que se proponen en la administración de riesgos, con lo que finalmente se podrá valorar de forma cualitativa y cuantitativa.
3. Información general acerca de la administración de riesgos de seguridad, capítulo en el que se analiza el proceso de administración de seguridad, en las que se considera el planeamiento y la creación del equipo de administración.
4. Evaluación del riesgo, en el que se analizan las etapas de planeación, identificación y valoración, pasando por la asignación de las prioridades a los riesgos.
5. Apoyo a la toma de decisiones, capítulo en el que sugiere actividades para que el equipo de administración de riesgos proponga soluciones eficaces, eficientes y asequibles, a cada amenaza identificada, además de la evaluación de los riesgos residuales que podrían presentarse.
6. Implementación de los controles y medición de la efectividad del programa, a manera de validar la efectividad del programa, vigilando, además, los cambios que se producen en el medio informático. (Microsoft, 2006) (Vásquez & López, 2016)

Actualmente, la metodología utiliza el modelo de defensa en profundidad, lo que permite al equipo de administración de riesgos de seguridad de la información, recopilar datos en el entorno organizacional, además de ofrecer una estructura adecuada. Estos niveles de defensa son presentados en el gráfico a continuación:

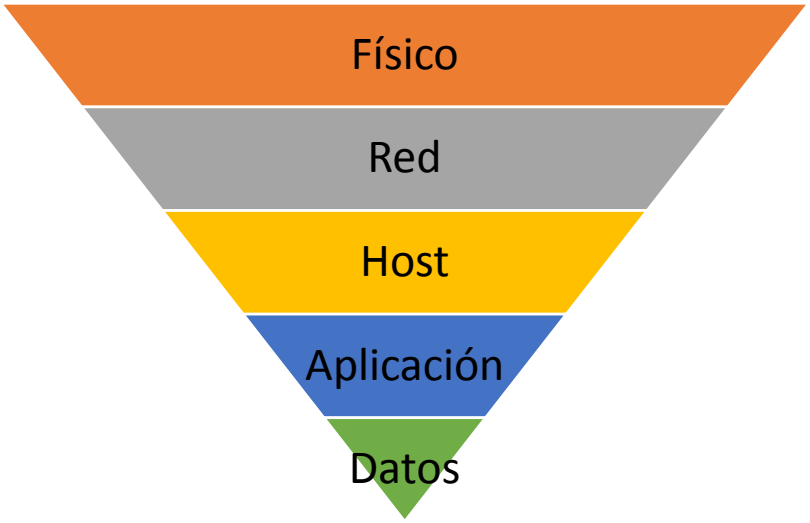


Ilustración 2: Principio de defensa en profundidad. Fuente: (Vásquez & López, 2016) Elaborado por: El autor

Se puede argumentar entonces, que la metodología Risk de Microsoft busca asegurar los activos de información de acuerdo a su categorización, partiendo de lo físico hasta llegar a lo lógico. Para ello, un equipo de trabajo participa en la planificación, diseño e implementación de un sistema de gestión de seguridad de la información, contemplando los riesgos y amenazas que podrían presentarse en el entorno en el que se desenvuelve la organización.

Magerit

Es una metodología desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, quien la ha definido como

> "*Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios*" (Ministerio de Hacienda y Administraciones Públicas de España, 2012) (Crespo & Cordero, 2016).

Por otro lado, Cordero acota que: "Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información, por lo tanto, se puede decir que es un instrumento que facilita la implantación y aplicación del esquema nacional de seguridad de España, proporcionando los principios básicos y requisitos mínimos para la protección de la información" (Cordero, 2015). Desde otro punto de vista, la gestión de riesgos consiste en el proceso de analizar, evaluar, tratar, monitorizar y comunicar los riesgos encontrados (Cocho, 2006).

La guía Magerit consta de tres tomos: el método, el catálogo de elementos, y la guía de técnicas. Para Crespo y Cordero, el ciclo de la metodología Magerit parte de la identificación de los activos de información, para por consiguiente identificar las amenazas lógicas y las de entorno, y luego estimar las frecuencias y el impacto, las mismas que servirán como insumo para la identificación de las salvaguardas, y así gestionar, como aspecto final, el riesgo residual (Crespo & Cordero, 2016) (Cordero, 2015).

Así mismo, Crespo y Cordero mencionan que Magerit considera como activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos. Magerit sugiere una escala de valoración de 1 al 10, donde 1 es insignificante y 10 es de muy alta importancia (Cordero, 2015) (Crespo & Cordero, 2016).

CRAMM

La metodología CRAMM (CCTA Risk Analysis and Management Method), fue desarrollada en 1985 en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones, cuyo objetivo era proteger la confidencialidad, integridad y

disponibilidad de un sistema de información y sus activos; y se la define como una metodología utilizada para el análisis y gestión de riesgos, orientada a proteger la confidencialidad, la integridad y disponibilidad de un sistema y sus activos, pudiendo ser aplicable a todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad; donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones (Yazar, 2002) (Cordero Torres, 2015) (Crespo & Cordero, 2016).

CRAMM, a su vez, consiste de tres fases: Identificación, análisis y evaluación de riesgos. La última versión identificada de la metodología, es la versión 5, liberada en el año 2003. Esta metodología recomienda el uso de entrevistas y cuestionarios estructurados para el levantamiento de información. En la fase inicial de recolección de datos, lo hace mediante entrevistas a los altos directivos de la organización, a manera de identificar los objetivos, el ámbito y los beneficios de la revisión, los términos de referencia, la estructura el proyecto, agenda y entregables, además de identificar entrevistas adicionales. Estos resultados deben ser documentados en el "Documento de inicialización del proyecto". (Yazar, 2002)

Según Yazar, las tendencias de un ataque vienen dadas por:

- La automatización, es decir, la velocidad de las herramientas de ataque y su incremental sofisticación
- La rapidez con la que se pueden descubrir vulnerabilidades
- El incremento en la filtración de firewalls e IDS
- El incremento de tretas asimétricas
- El aumento de vulnerabilidades debido a los ataques de infraestructura.

CRAMM calcula el riesgo en base a una valoración de las vulnerabilidades, realizada mediante una escala del 1 al 7, utilizando una matriz de riesgos con valores predefinidos, dados por la comparación del valor de los activos frente a los niveles de tretas y vulnerabilidades, donde 1 significa un bajo requerimiento de seguridad y 7 un alto requerimiento. La metodología puede reportar los hallazgos que deben ser presentados a la administración para acordar y aprobar el proceder con la fase de gestión de riesgo. En esta

etapa, se requiere establecer una entrevista con la gerencia para concentrar los esfuerzos en priorizar soluciones sobre las áreas con mayor nivel de vulnerabilidades (Yazar, 2002).

Yazar menciona que CRAMM cuenta con una extensa lista de contramedidas (cerca de 4000), que han sido recolectadas y clasificadas en grupos y sub grupos: hardware, software, comunicaciones, procedimientos, elementos físicos, personal y entorno. Cada contramedida ha sido marcada con un nivel de seguridad de 1 (muy baja) a 7 (muy alta), que es seleccionada por la comparación de la medida de riesgo. Uno de los puntos fuertes de CRAMM es la asistencia en la priorización que se le debe dar a una contramedida, considerando que debe ser de alta prioridad si:

- Esta protege a los activos de información de muchas tretas
- Si protege a un sistema de alto riesgo
- Si no existen contramedidas alternativas actualmente instaladas
- Las que son menos costosas de implementar
- Si es más efectiva en identificar los objetivos de su sub grupo
- Si previene un incidente más que detectarlo o facilita su recuperación (Yazar, 2002).

CRAMM no incluye una revisión detallada o una operación efectiva de las contramedidas. La última opción en implementar, mejorar o remover las contramedidas son responsabilidad absoluta de los administradores. La fecha en el que la siguiente revisión debe ser realizada debería estar de acorde con los requerimientos del negocio, las configuraciones del sistema, y las vulnerabilidades y tretas que pueden presentarse, las mismas que probablemente pueden cambiar (Yazar, 2002).

Octave – S

Según Vásquez y López, citando a Ana y John A. (2013), *"La metodología OCTAVE evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. Equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que, a partir de estos, los entes empresariales puedan tomar*

decisiones de protección de información basados en los principios de la seguridad de la información."

Así también mencionan que OCTAVE es una metodología que se enfoca en las actividades diarias de las organizaciones, partiendo de la identificación y valoración de los activos de información, como cualquiera de las otras metodologías que persiguen este fin. Además, busca dar a conocer la importancia de que cada uno de los miembros de la organización conozcan sobre la importancia de estos activos, y de los riesgos que implica la actividad de las amenazas de entorno.

Vásquez y López mencionan que "Para realizar el estudio se debe crear un grupo conformado por personas de las áreas de negocio y del área de TI (Tecnología de la Información), llamado por OCTAVE **"el equipo de análisis""**. Además, consideran que este grupo es fundamental, debido a que, al contar con un adecuado equipo de trabajo, se podrán identificar de una manera ágil y oportuna los activos de información más relevantes, además de que permitirán conocer a ciencia cierta sobre las debilidades y vulnerabilidades que pueden presentarse sobre los mismos (Vásquez & López, 2016).

Para realizar la identificación de la información, el equipo de análisis conformado deberá dividir al proceso en tres fases:

1. Construir perfiles de amenaza de activos, describiendo los requerimientos de seguridad para lograr construir un perfil de amenazas para cada uno de los activos identificados como críticos. (Vásquez & López, 2016). Luego de esto, y de acuerdo con Gómez, Pérez, Donoso y Herrera, 2011, se deberán verificar aspectos como la completitud, la coherencia y las diferencias de apreciación en cada uno de los niveles de la organización. El resultado de esta fase se resume en haber logrado la identificación de los activos críticos y los requerimientos de seguridad que permitirán mitigar las amenazas detectadas.

OCTAVE, por naturaleza, identifica solamente cuatro categorías principales de amenazas: Problemas debido al acceso a través de la red, errores por acceso físico, problemas del sistema y otros problemas.

2. Identificar las vulnerabilidades en la infraestructura

   En esta etapa, el equipo deberá evaluar cada uno de los distintos componentes organizacionales, con el objetivo de identificar vulnerabilidades tecnológicas, que habilitarían las acciones sin autorización en contra de los activos críticos.

   Los resultados de esta etapa se resumen en componentes clave (relacionados con los activos críticos), que, según Vásquez y López, serían los firewall, servidores, enrutadores y sistemas de almacenamiento de información; y como un segundo resultado, las vulnerabilidades tecnológicas actuales que mantiene la empresa, producto del escaneo con herramientas como OPENVAS, NESSUS o LANGUARD.

3. Desarrollar planes y estrategias de seguridad

   Luego de haber identificado los riesgos existentes sobre los activos de información críticos, el equipo de trabajo planifica y desarrolla políticas de mitigación de riesgos, basados en la información adquirida en las etapas anteriores. Resultados de este proceso son los riesgos valorados en una escala de tres niveles: alto, medio y bajo; así como también las estrategias de protección y los planes de mitigación del riesgo.

Vásquez y López, en su trabajo de investigación, acotan que la metodología OCTAVE está enfocada en las grandes empresas. También mencionan que esta metodología se divide en dos sub metodologías: OCTAVE Allegro que está enfocada al análisis de riesgos, considerando en amplitud los activos de información; y OCTAVE-S que es la metodología enfocada a las pequeñas empresas (Vásquez & López, 2016).

Conclusiones del capítulo 2

Una vez revisadas las metodologías CRAMM, Magerit, Microsoft Risk Management y Octave, se puede concluir que, en primera instancia, la metodología más sencilla de manejar es la de Microsoft. Sin embargo, se debe acotar que ésta se encuentra más orientada a la seguridad informática, pues el nivel y profundidad con la que clasifica los activos de información es bastante limitado.

La guía Microsoft Risk Management tiene la ventaja de que, para un entorno latinoamericano, se encuentra escrita en lenguaje español. Coincidiendo con (Vásquez & López, 2016), Microsoft Risk Management es en sí, una alternativa viable desarrollada por: técnicos, clientes y especialistas computacionales cuyo fin es el de crear conciencia sobre los posibles riesgos informáticos, su valoración cuantitativa y cualitativa, así como el planteamiento de un esquema de investigación y gestión de riesgos que será ejecutado en cada una de las organizaciones. Cada empresa deberá contar con una plantilla que servirá para la recolección de datos, Dentro de las empresas debe existir una plantilla de recolección de datos de los activos la cual, ayudará a gestionar información, facilitar estudios y análisis.

En su tesis de grado, (Vásquez & López, 2016) mencionan que Octave-S se basa en 3 fundamentos clave: La identificación de activos de información críticos y sus amenazas, la identificación de las vulnerabilidades, y el desarrollo de estrategias y planes de seguridad.

Magerit V3 por su lado contiene, en el tomo 2 (catálogo de elementos), las plantillas con los elementos de identificación que sugiere ser utilizados en cada una de las fases de identificación de riesgos. La guía es muy clara y también se encuentra escrita en idioma español, y su última actualización es en el 2012. Además, ofrece la sintaxis XML para el intercambio de información entre plataformas. La desventaja de la metodología

A cerca de CRAMM, actualizada por última vez en el año 2009, se puede decir que no es una metodología de acceso gratuito y está disponible únicamente en idioma inglés, pero contiene una guía muy detallada sobre planificación, procesos y elementos a considerar en la identificación de activos, amenazas y riesgos. El punto débil es que, al ser demasiado

extensa, se enfoca más a las grandes empresas, además de dejar de lado el principio de no repudio; por cuanto no sería aplicable directamente a una MPYME. Está basada en el contexto británico, por cuando quedaría muy lejos de la realidad ecuatoriana.

De cualquier forma, para todas las metodologías, la información de cada uno de los activos, amenazas y riesgos, es recolectada en plantillas y matrices. Risk y Octave-S servirá para planificación de reuniones futuras, en donde el reto consistirá en diseñar un efectivo plan de políticas de seguridad, el mismo que permita mitigar los riesgos que pueden presentarse y afectar a cada una de las dimensiones valoradas de los activos de información.

Risk, al igual que Octave-S, sugiere que las reuniones deben estar basadas en debates direccionados, considerando actividades de control y monitoreo efectivo y permanente del sistema informático, y que finalizará con evaluaciones dadas por cada uno de los participantes. En cada una de estas, deberá asistir todo el personal que sea responsable de la información (dueño de información) de una empresa, con el objetivo de identificar aspectos de riesgo operativo y tecnológico. Además, consideran que es importante el manejo de terminologías desconocidas o aspectos que no forman parte de la organización mediante un lenguaje más general y asimilable.

Todos y cada uno de los miembros a que sean partícipes del proceso de identificación de riesgos de seguridad y que puedan dar, como resultado, indicadores que permitan valorar la posible probabilidad de riesgo de una manera cualitativa, es decir, alta, media y/o baja, a la que finalmente se le deberá hacer un adecuado seguimiento.

Se habla también de una escala de riesgos que involucra a los activos tangibles e intangibles, los mismos tienen un valor específico que está dado por un rango y una clasificación determinada. El primero hace referencia al daño o afección que pueden sufrir tanto los equipos como la información, posteriormente el segundo trata la probabilidad de que ocurra y a los efectos que causan los riesgos para organización.

Octave por su lado, solo incluye una exploración limitada de la infraestructura informática. (Vásquez & López, 2016) acotan que "*las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad*".

Indistintamente de su autor o marca, cada una de las metodologías estudiadas están basadas en las normas ISO que apoyan en la gestión de seguridad de la información y el riesgo. Toma de cada una de ellas los aspectos más relevantes en cada uno de los procesos que conforma un sistema de gestión de seguridad de la información SGSI; esto es, la identificación y valoración de los activos de información, la identificación y valoración de vulnerabilidades y amenazas, el cálculo de riesgo y el establecimiento de alternativas de mitigación.

De todas las guías gratuitas, MAGERIT es la más completa, pues implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Según la guía Magerit, el análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, siendo esta la piedra angular que permite controlar todas y cada una de las actividades con fundamento. La fase de tratamiento de riesgos estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis, que concluyen en cuatro etapas cíclicas: Planificación, implementación y operación, monitorización y evaluación, y mantenimiento y mejora.

Toda metodología sugiere partir de la creación de conciencia sobre los riesgos de información en la institución, para luego desarrollar políticas corporativas de fácil interpretación, que aclare obviamente el uso correcto e incorrecto de cada uno de los activos de información, y que se la realice permanentemente mediante elementos informativos como son las carteleras, la Intranet, así como la capacitación continua a todos

los niveles, recordando cuidados rutinarios y actividades especializadas, que inciden en la responsabilidad de cada uno de los involucrados.

Risk, Octave-S y Magerit son metodologías que están al alcance de cualquier organización de forma gratuita, acotando que la última versión de Risk fue en el año 2006, y la última actualización de Magerit en el 2013. Por su simplicidad, cualquiera de estas metodologías podría ser adoptadas por las organizaciones, empresas e instituciones del sector MPYME, especialmente la primera.

Capítulo 3: Alineación de las metodologías con las normas ISO

Para que una metodología sea efectiva, debe estar alineada con los estándares y mejores prácticas de la industria. El presente capítulo permite identificar la alineación de cada una de las metodologías estudiadas y las normas ISO: 27001, 27002, 27005 y 31000, utilizadas en la gestión de seguridad de la información y en la gestión de riesgos.

Microsoft Risk Management

La guía metodológica creada por Microsoft cuenta con 4 dominios macro, los mismos que, según Vásquez y López, consisten en:

1. Identificación de activos
2. Gestión del riesgo
3. Apoyo a la toma de decisiones
4. Evaluación de efectividad

En el trabajo realizado por (Vásquez & López, 2016), se determina que para los procesos que conforman el dominio de identificación de activos: Identificación de activos y valoración de activos, respectivamente; el primer proceso se alinea con la ISO 27001 en la identificación de activos que los clasifica en dos grupos (hardware y software), además de su alineación con la ISO 27005, relacionada con la identificación de activos, en la que sugiere la creación de un ámbito de gestión de los mismos.

Relacionados con el proceso de valoración de activos, Risk toma aspectos de la ISO 27001 en cuanto a la identificación e inventariado de los activos; de la ISO 27002 en lo referente a parámetros de clasificación en términos de valor, requisitos legales, sensibilidad y criticidad de la organización; y de la ISO 27005 en cuanto al establecimiento de criterios para la valoración de los activos (Vásquez & López, 2016).

Del segundo dominio, gestión de riesgos, según (Vásquez & López, 2016), se desprenden los siguientes procesos:

1. Identificación de riesgos

2. Valoración del riesgo
3. Impacto en la organización
4. Definición de vulnerabilidades
5. Definición de amenazas

El proceso de Identificación de riesgos toma de la ISO 27001 las mejores prácticas para la identificación de los riesgos y de los lineamientos para los controles de mitigación; de la ISO 27002 adopta los requerimientos para evaluación y tratamiento de riesgos; de la ISO 27005 indica los lineamientos y metodología para implementar una lista de priorización de riesgos de acuerdo con los criterios de evaluación, en relación a los escenarios que conducen a los mismos; y de la ISO 31000, concibe procedimientos para la identificación de las fuentes de riesgo, el desarrollo de una lista minuciosa de eventos que podrían presentarse y afectar a la institución en el alcance de sus objetivos, además de las consecuencias que podrían presentarse (Vásquez & López, 2016).

En cuanto al proceso de valoración de riesgos, (Vásquez & López, 2016) coinciden en que de la ISO 27001 establece los parámetros para la definición del enfoque de la evaluación de riesgo; de la ISO 27002 recoge las mejores prácticas para la identificación, cuantificación y priorización de los riesgos; de la ISO 27005 define la escala de valoración de riesgo en alta, media y baja; y de la 31000 adopta las mejores prácticas para el tratamiento del riesgo de información.

Sobre el proceso "Impacto a la organización" en el que lo clasifica en Alto, medio o bajo; (Vásquez & López, 2016) argumentan que de la ISO 27001 recoge los lineamientos para la adecuada identificación de impactos, considerando las pérdidas de integridad y disponibilidad de los activos; de la ISO 27002, incluye procedimientos para la evaluación de riesgos, análisis de impactos y la especificación de los controles de seguridad necesarios; y de la ISO 27005 adopta las sugerencias para la asignación de prioridades a los riesgos.

En referencia al proceso de definición de vulnerabilidades, la ISO 27001 proporciona los lineamientos para el control de vulnerabilidades técnicas, la ISO 27005 adopta los métodos

de evaluación de vulnerabilidades; y de la ISO 31000 los procedimientos para la identificación de riesgos, considerando la adecuada identificación de los mismos, considerando causas y escenarios posibles.

En cuanto al proceso de definición de amenazas, (Vásquez & López, 2016) sugieren que la metodología Risk Management se apoya en la ISO 27001 en cuanto a la protección contra amenazas externas y ambientales; en la ISO 27002 debido a que recoge las mejores prácticas para la coordinación de seguridad de la información; de la ISO 27005 asume los ejemplos de las amenazas típicas; y de la ISO 31000, de igual manera que en el proceso anterior, conoce los procedimientos que se utilizan en la identificación y valoración de los riesgos, en cuanto a las causas y escenarios posibles.

El tercer dominio de la metodología, Apoyo a la toma de decisiones, está conformado por los siguientes procesos:

1. Proceso de respuesta a incidencias
2. Definición de requisitos
3. Identificar soluciones de control
4. Revisar soluciones propuestas
5. Establecer política de seguridad
6. Cálculo de la reducción de nivel de riesgo
7. Cálculo del coste de cada solución
8. Selección de estrategia de mitigación de riesgos

Para primer proceso, la ISO 27001 proporciona una lista denominada "Lista de objetivos de control y controles"; la ISO 27002 establece las pautas que permiten ejecutar la lista de objetivos de control y controles; y la ISO 31000 proporciona las directrices para que los controles puedan ser correctamente diseñados y operados, obteniendo información adicional para mejorar la valoración del riesgo, e identificando los riesgos emergentes.
Para el proceso “definición de requisitos”, (Vásquez & López, 2016) argumentan que la ISO 27001 apoya a la metodología brindando los lineamientos que apoyan al tratamiento de seguridad de las amenazas identificadas, antes de otorgar acceso a la información o activos

de la organización; la ISO 27002 detalla la manera de organizar la seguridad de la información; y la ISO 31000 apoya en los lineamientos para establecer el contexto, en el cual se incluyen las metas y objetivos, las responsabilidades y la definición del alcance.

El proceso de identificación de soluciones de control, la ISO 27001 brinda las pautas para seleccionar los controles a utilizar para el tratamiento de los riesgos, la ISO 27002 proporciona los procedimientos de desarrollo, emisión, aprobación, implementación y seguimiento de las políticas de seguridad de la información; la ISO 27005 sugiere las dos formas de soluciones de control (preventiva y correctiva) que conllevan al mejoramiento de la calidad de la gestión de riesgos; y la ISO 31000 proporciona las pautas para el monitoreo y revisión, además de la identificación de riesgos emergentes (Vásquez & López, 2016).

Para el proceso de revisión de soluciones propuestas, la ISO 27001 sugiere que la política de seguridad debe ser evaluada en intervalos de tiempo regulares, o en cada cambio significativo; la ISO 27002 hace referencia al documento de políticas de seguridad de la información, mantiene los procedimientos de desarrollo, emisión, aprobación, implementación y seguimiento; la ISO 27005 por su lado sugiere que todas las soluciones de control deben ser revisadas por el equipo de administración de riesgos de seguridad de la organización, lo que permitirá establecer correctamente los costos y beneficios de las soluciones identificadas; y la ISO 31000 proporciona las directrices para controles que deben ser utilizados en el monitoreo y revisión de las políticas y contramedidas implementadas (Vásquez & López, 2016).

Para establecer la política de seguridad, la ISO 27001 proporciona las directrices que habilitan la documentación de las políticas de seguridad de la información; la ISO 27002 recomienda los procedimientos de desarrollo, emisión, aprobación, implementación y seguimiento a utilizar; la ISO 27005 establece los mecanismos para evitar los riesgos, y la ISO 31000, al igual que en el proceso anterior, proporciona las directrices para controles que deben ser utilizados en el monitoreo y revisión de las políticas y contramedidas implementadas (Vásquez & López, 2016).

El proceso de cálculo de la reducción de nivel de riesgo, la ISO 27001 proporciona las directrices para el monitoreo y la gestión de riesgos, sugiriendo que los mismos deben contemplar intervalos de revisión, además del cálculo de riesgo residual; la ISO 27002 sugiere el tratamiento de los riesgos de seguridad y los procedimientos para poder lograrlo; la ISO 27005 establece directrices para el tratamiento de la reducción de riesgo y su evaluación constante; y la ISO 31000 sugiere los procedimientos para el tratamiento de gestión de riesgo (Vásquez & López, 2016).

Para el procedimiento que hace referencia al cálculo del coste de cada solución, la ISO 27001 sugiere que deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de información; la ISO 27002 explica la manera de calcular costo de la implementación y operación en relación con los riesgos que se reducen, y del resto proporcional a los requisitos y limitaciones de la organización; la ISO 31000 sugiere los procedimientos para el tratamiento de gestión de riesgo (Vásquez & López, 2016).

En cuanto al proceso que permite seleccionar la estrategia de mitigación de riesgos, la ISO 27001 apoya a la fase "Hacer" del ciclo de Deming, ya que según (Vásquez & López, 2016), abarca la implementación y uso operacional de esos controles; la ISO 27005 explica detalladamente el proceso llamado "tratamiento de riesgos", que incluye la retención, reducción y transferencia de riesgos; y, al igual que en el proceso anterior, la ISO 31000 sugiere los procedimientos para el tratamiento de gestión de riesgo.

El cuarto dominio, Evaluación de efectividad, según (Vásquez & López, 2016), comprende los siguientes procesos:

1. Cálculo de riesgo residual
2. Medir la efectividad del control

Para el primer y segundo proceso, según (Vásquez & López, 2016), de la ISO 27001 considera las prácticas que revisa las evaluaciones del riesgo obtenidas por intervalos

planeados, además de monitorear el nivel de riesgo residual y aceptable, identificando los cambios producidos en la organización, la tecnología, los procesos comerciales, las amenazas identificadas, y la efectividad de controles implementados; de la ISO 27002 asume las mejores prácticas relacionadas con los mecanismos de protección de activos críticos que apoyan a las actividades esenciales de negocio; de la ISO 27005, recoge las mejores prácticas que sugieren la documentación de controles y planes de implementación para el tratamiento del riesgo; y finalmente, de la ISO 31000, evalúa las prácticas que permiten tratar el riesgo y establecer los procedimientos y controles que habilitan el monitoreo continuo de las actividades de gestión.

Octave – S

(Vásquez & López, 2016) identifican tres dominios para la metodología Octave – S, los mismos que se resumen de la siguiente manera:

1. Construir perfiles de amenazas basados en activos.
2. Identificar vulnerabilidades de la infraestructura
3. Desarrollo de estrategias y planes de seguridad

El primer dominio, Construir perfiles de amenazas basados en activos, considera, según (Vásquez & López, 2016), los siguientes procesos:

1. Identificar la información organizacional
2. Crear perfiles de amenaza

El primer proceso, incluye la definición de un rango de potencial impacto (alto, medio, bajo), en áreas como: confianza de los clientes, financiera, seguridad personal, sanciones, productividad y sistemas informáticos. Aquí, la ISO 27001 brinda las pautas para identificar el impacto que puede afectar a la integridad, disponibilidad e integridad sobre un activo de información; la ISO 27002 sugiere que el proceso debe incluir una evaluación de

riesgos, el análisis de los impactos de los cambios, y la especificación de los controles de seguridad necesarios; y la ISO 27005 proporciona los mecanismos para la identificación de activos de información y los riesgos, además de la evaluación de los mismos.

Para el segundo proceso del primer dominio, la ISO 27001 habilita los procedimientos para la identificación de activos de información en dos grupos: Hardware y Software, por otro lado, sugiere políticas para la identificación de riesgos y para la protección de los activos contra las amenazas de entorno; la ISO 27002, proporciona directrices para la evaluación y tratamiento de riesgos, además de sugerencias para la coordinación de la seguridad de la información; la ISO 27005 brinda los criterios que deben considerarse para la identificación de amenazas, además de la evaluación del riesgo; y la ISO 31000 da a conocer las mejores prácticas de la industria que deben ser utilizadas en la identificación de los riesgos.

El segundo dominio, Identificar vulnerabilidades de la infraestructura, según (Vásquez & López, 2016), incluye el siguiente proceso:

1. Examinar la infraestructura computacional en relación con los críticos activos.

Para este proceso, según Vásquez y López, la ISO 27001 establece que toda la información y los activos asociados con los medios de procesamiento de la información deben ser propiedad de un parte designada de la organización; por otro lado, la ISO 27002 sugiere que los puntos débiles de seguridad deben ser reportados por todos los miembros directos o indirectos de la institución; y la ISO 27005, adicionalmente, proporciona la lista de amenazas conocidas, la lista de los activos y los controles existentes, ayudando a la identificación de vulnerabilidades.

El tercer dominio, Desarrollo de estrategias y planes de seguridad, según (Vásquez & López, 2016), incluye los siguientes procesos:

1. Identificar y analizar los riesgos.
2. Desarrollar estrategias de protección y planes de mitigación

Para el primer proceso, según (Vásquez & López, 2016), Octave – S toma de la ISO 27001 las mejores prácticas para determinar el impacto que pueda ser consecuencia de la pérdida de integridad, confidencialidad y disponibilidad de los activos de información; de la ISO

27002 concibe las recomendaciones acerca de incluir una evaluación de riesgos, el análisis de los impactos de los cambios, y la especificación de las contramedidas o controles necesarios; y de la ISO 27005 toma la recomendación de asignar prioridades a los riesgos.

En cuanto al segundo proceso de este tercer dominio, Vásquez y López sugieren que esta metodología toma de la ISO 27001 los procedimientos para la planificación y selección de los controles para el tratamiento de riesgos, además de controlar los cambios en los medios y sistemas de información, y la revisión constante a las políticas de seguridad de la información; de la ISO 27002 hace referencia al documento de políticas de seguridad de la información, en cuanto a los procedimientos de desarrollo, emisión, aprobación, implementación y seguimiento; las recomendaciones de gestión de cambio y al monitoreo constante de las políticas de seguridad de la información. De la ISO 27005 considera las mejores prácticas recomendadas para el monitoreo y revisión de los factores de riesgo, además de sugerir que todas las soluciones de control deben ser revisadas por el equipo de administración de riesgos de seguridad de la organización con el fin de establecer costos y beneficios de las soluciones. Finalmente, de la ISO 31000, adopta las sugerencias y controles que deben utilizarse para el monitoreo y revisión, en el cual busca garantizar la eficacia y eficiencia de los controles, elementos que deben considerarse para mejorar la valoración del riesgo, aprender de la experiencia obtenida; y detectar cambios en el contexto interno y externo, que puedan exigir revisión de los tratamientos del riesgo y su asignación de prioridades.

Magerit

La metodología española creada por el Ministerio de Hacienda comprende los siguientes dominios:

1. Identificación y valoración de activos
2. Identificación y valoración de amenazas
3. Cálculo de riesgo
4. Identificación de las contramedidas
5. Cálculo de riesgo residual

El primer dominio de la metodología Magerit comprende los siguientes procesos

1. Identificación de los activos de información
2. Valoración de los activos

El primer dominio, según (Cordero Torres, 2015) y (Crespo & Cordero, 2016), la ISO 27001 recomienda clasificar los activos como software y hardware, que son claramente identificados y clasificados considerando su sentido de su valor, sensibilidad y de criticidad a la organización. Citando al Portal de Administración pública de España, (Cordero Torres, 2015) sugiere que, dentro de la clasificación de los activos de información, se puede identificar: red telefónica, red digital, red de datos, punto a punto, comunicación de radio, red inalámbrica, telefónica móvil, por satélite, red local, red metropolitana e internet. La ISO 27005 por su lado, sugiere la creación de un ámbito de gestión de los mismos.

El segundo dominio de la metodología Magerit comprende los siguientes procesos

1. Identificación de las amenazas
2. Valoración de las amenazas

Para estos procesos, la ISO 27002 sugiere directrices para establecer los parámetros de clasificación en términos de valor, requisitos legales, sensibilidad y criticidad de la organización, acotando que los criterios de clasificación establecidos por la norma las son fáciles de identificar, e indica además el tipo de activos que pueden verse afectados, dando a conocer la disponibilidad o dimensión de la misma. Estas amenazas pueden ser de índole natural, origen industrial, error y fallos no intencionados, ataques intencionados y nuevas amenazas. La ISO 27005 por su lado, brinda procedimientos y lineamientos para identificar las amenazas que pudiesen alterar o dañar los activos de información, atacando las vulnerabilidades existentes; mientras que la ISO 31000 proporciona los procedimientos necesarios para la identificación de riesgos, considerando la adecuada identificación de los mismos, reflexionando sobre causas y escenarios posibles.

El tercer dominio de la metodología Magerit comprende los siguientes procesos

1. Cálculo de riesgo e impacto

En este dominio, Magerit se apoya en la ISO 27001 debido a que en la sección D de esta normativa, indica el procedimiento a seguir para determinar el impacto que se puede tener cuando los factores de integridad, confidencialidad y disponibilidad se ven comprometidos. En cuanto a la ISO 27002, se alinea con esta normativa debido a que recoge las mejores prácticas para la evaluación de riesgo y cálculo de impacto; y de la ISO 27005, los criterios para la evaluación de riesgos.

El cuarto dominio de la metodología Magerit comprende los siguientes procesos

1. Identificación contramedidas
2. Priorización de las contramedidas

La metodología Magerit adopta las mejores prácticas de la ISO 27001 en cuanto a la identificación de alternativas de mitigación, conocidas como contramedidas en la metodología estudiada, la ISO 27001 sugiere que, una vez completada la fase de evaluación del riesgo, se deben seleccionar los controles para el tratamiento de los riesgos como una etapa de la fase de planificación, en los que se deben tratar todos los consideraciones de vulnerabilidad y amenazas identificadas, antes de otorgar acceso a la información o activos de la organización.

CRAMM

A pesar de que (Cordero Torres, 2015) argumenta que la metodología CRAMM, debido a su amplitud y acceso restringido por el costo, es utilizada especialmente en las grandes empresas, quedando fuera del sector MPYME que es el que se está analizando, en la siguiente sección se procede a evaluar su alineación con las metodologías ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

CRAMM, de acuerdo con el estudio realizado por (Cordero Torres, 2015), considera tres dominios o etapas macro:

1. Identificación y valoración de activos
2. Evaluación de los requisitos para la identificación de riesgos y amenazas
3. Contramedidas

Dentro de la etapa de identificación y valoración de activos, CRAMM realiza los siguientes procedimientos:

1. Definición del límite de estudio
2. Identificación y valoración de los activos físicos
3. Identificación y valoración de los activos lógicos

En esta etapa o dominio, la metodología al igual que la ISO 27001, realiza un inventario de activos de información, ya sean estos de software, hardware e infraestructura física que brinda soporte a las tecnologías de información y comunicaciones. El estándar clasifica sus activos mediante software, hardware. Estos activos que se han identificado, posteriormente serán clasificados de acuerdo a su sentido de valor, la sensibilidad, y la criticidad con respecto a la organización. Citando a Manuel Fernández, Cordero menciona que tanto el estándar como la norma busca proteger los activos y que estos cumplan con las normas de confidencialidad y trazabilidad.

Dentro de la etapa de identificación y valoración de riesgos, CRAMM realiza los siguientes procedimientos:

1. Identificación y valoración de las amenazas
2. Calculo de medidas de riesgo

La ISO 27001, aporta a la metodología en cuanto a procedimientos que permitan identificar las amenazas y el impacto que se produciría si una vulnerabilidad es explotada.

Según (Cordero Torres, 2015), la alineación de CRAMM con la ISO 27002 es notoria y relevante al momento de identificar y cuantificar las amenazas. Una vez detectado el problema potencial, analiza la probabilidad de ocurrencia. Cubre toda la gama de amenazas

deliberadas o accidentales que puedan afectar a los sistemas de información, incluyendo hacking, virus, fallos de equipo o software, daños intencionales o el terrorismo y errores humanos.

La alineación de CRAMM con la ISO 27005, según (Cordero Torres, 2015), se da en la identificación de amenazas, vulnerabilidades, obtenidas a partir del análisis de activos, incidentes y catálogos de amenazas externas. Además, citando a Juan Manuel Matalobos, Cordero acota que la metodología CRAMM se alinea con el estándar ISO 27005 en su fase de planificación, donde se realiza la identificación y evaluación del riesgo.

En la etapa de identificación de contramedidas, CRAMM contempla los siguientes procedimientos:

1. Plan de seguridad
2. Estrategias

Es en este dominio donde CRAMM adopta las mejores prácticas de la ISO 31000, ya que, en esta fase, el estándar sugiere la implementación de contramedidas. La metodología tiene procedimientos que permiten evaluar la relevancia de los riesgos, a manera de determinar si vale la pena implementar contramedidas. En cuanto a la ISO 27001, hace referencia a la gestión del cambio, y al establecimiento de contramedidas, específicamente en el documento de políticas de seguridad. De la ISO 27002 adopta los procedimientos de desarrollo, emisión, aprobación, implementación y seguimiento del documento de políticas de seguridad de la información. En cuanto a la ISO 27005, toma las recomendaciones en cuanto al monitoreo continuo de los factores de riesgo, en una etapa temprana.

Conclusiones del capítulo

Luego de desarrollado este capítulo, se ha podido ver claramente que las normas ISO influyen directamente en cada una de las etapas que contemplan las metodologías

estudiadas. Las ISO 27001 y 27002 comprenden las mejores prácticas para establecer un ciclo de gestión de seguridad de la información, mientras que el aporte indiscutible sobre la gestión de riesgos está dado por las normas ISO 27005 e ISO 31000.

Básicamente, cada metodología comprende cuatro etapas elementales:

La primera etapa comprende los activos de información, que incluye las actividades de identificación de activos de información y su valoración cualitativa, considerando al menos tres criterios para este propósito: Confidencialidad, Disponibilidad e Integridad. Magerit, por ejemplo, requiere considerar además de estos tres criterios, la Autenticidad, es decir garantizar que el acceso al activo de información se da por un usuario o sistema auténtico; y la Trazabilidad, que consiste en dejar rastros sobre el sistema o persona que mantuvieron acceso a un activo de información.

La segunda etapa comprende las amenazas. Aquí cada metodología busca identificar las amenazas físicas o de entorno, y las lógicas que podrían afectar a la disponibilidad, confidencialidad o integridad de la información. Es importante considerar que cada una de las metodologías utiliza criterios de valoración cualitativas, en algunos casos en tres niveles (alto, medio, bajo), o, en el caso de Magerit, una escala en 10 niveles, desde irrelevante hasta muy importante.

La tercera etapa es el cálculo del riesgo basado en el impacto que podría ocasionar una amenaza sobre la vulnerabilidad que presenta un activo de información. Cada metodología adopta las prácticas de las ISO 27005 e ISO 31000 para realizar tal tarea. Una vez que cierra esta etapa, procede con la siguiente.

La cuarta etapa consiste en aplicar mecanismos de mitigación de riesgos, conocidos también como salvaguardas o contramedidas. Estas, obviamente, deben ser objetivas, realizables y deben estar, sobre todo, alineadas a los requerimientos organizacionales, y dependen mucho de la valoración que han recibido los activos de información en la primera etapa.

El ciclo se cierra con el cálculo del riesgo residual, es decir, una vez que se han identificado las contramedidas, se calcula el impacto del riesgo contra su mitigación. Por ejemplo, si la contramedida ante una amenaza de virus, fue un antivirus; el riesgo residual se presentaría

si la herramienta no es actualizada de la forma requerida, quedando aun una probabilidad de que el equipo informático se infecte.

Capítulo 4: Marco Legal

Citando la frase de Aung San Suu Kyi *"La verdadera medida de la justicia de un sistema es la cantidad de protección que garantiza a los más débiles"*, el presente capítulo pretende analizar el entorno legal que hace referencia a la protección de datos y a la gestión de riesgos, partiendo de aspectos internacionales generales para luego analizar los aspectos de regulación en el Ecuador.

Delito Informático

Según (Borghello, 2009), la Organización de Naciones Unidas (ONU) reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras
2. Manipulación de los datos de entrada
3. Daños o modificaciones de programas o datos computarizados

(Borghello, 2009) menciona además que *"el delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho".*

Los criminales informáticos, según (Cano, 2009), responden a tipos de perfiles de personas o grupos que tienen en común un gusto y pasión por las tecnologías y sus posibilidades, quienes, aprovechando el alto desconocimiento de los habitantes comunes de una población, diseñan estrategias para lograr los objetivos ilícitos, vulnerando derechos y garantías establecidas por el marco legal en cuanto al uso de las tecnologías de información.

Al encontrar una vulnerabilidad, diversos propósitos pueden pasar por la mente del atacante. En la vida profesional, se puede ver que algunos buscan desde el simple apoderamiento de la sesión en una cuenta de correo electrónico, hasta el robo de millones de dólares en una cuenta bancaria, o la comercialización de una base de datos de clientes y referencias comerciales en el mercado negro. Es importante considerar el análisis del comportamiento humano, basado muchas veces en aspectos psicosociales, los cuales derivan en actos criminalísticos. (Cano, 2009), citando a (Soria 2006, p. 365), menciona que encuentra dificultades para distinguir los posibles delincuentes con inclinación al uso de las tecnologías, de otros con problemas por adicción al tema tecnológico.

Es en este escenario en el que las metodologías de gestión de riesgo facilitan a los administradores de tecnología, o los gestores de riesgo empresarial, a identificar la información que mantiene la institución, a valorarla, y a identificar los escenarios de amenazas, así como la manera de protegerla, considerando indudablemente las leyes que rigen el uso de tecnologías de información, protección de datos, divulgación, cesión de derechos, propiedad intelectual, entre otras.

(Borghello, 2009) citando a Julio Téllez Valdéz, los delitos se clasifican en dos categorías

1. Como instrumento o medio: que engloba a las conductas delictivas en las cuales las computadoras son el método, medio o símbolo en la comisión del ilícito. Bajo esta categoría, se puede ejemplificar la falsificación de documentos de manera electrónica, como, por ejemplo, la alteración de una cédula, cheques, tarjetas de crédito; la alteración de la situación contable de una empresa; la intervención de líneas de comunicación bajo la técnica de MITM (Hombre en el medio); o la alteración de un sistema mediante la intrusión de virus o código maligno.
2. Como fin u objetivo: en la que se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Bajo esta categoría se pueden incluir las instrucciones utilizadas para la negación de un servicio informático, destrucción de aplicaciones o programas por cualquier método; atentado a un cajero automático o al computador; secuestro o hurto de

medios ópticos o magnéticos para utilizarlo posteriormente en actividades delictivas.

Según (Borghello, 2009) citando a (Lima, 1984), el delito electrónico está clasificado de la siguiente manera:

1. Como Método: Donde las personas utilizan los métodos electrónicos para llegar a un resultado ilícito.
2. Como Medio: Considera que una computadora es utilizada como medio para efectuar un delito.
3. Como Fin: Son aquellas conductas criminales dirigidas contra la entidad física del objeto, máquina electrónica, o su material, con objeto de dañarla.

En resumen, se puede ver que, en cualquiera de los casos, en especial en este nuevo siglo, se utilizan los medios electrónicos para lograr resultados ilícitos, muchas veces alterando la información contenida en ellos, o bien utilizándolas para alcanzar otros fines, como por ejemplo lo sucedido en el caso Wikileaks, cuando la información contenida en ellos no fue alterada sino publicada; o casos que suceden comúnmente en las instituciones financieras, como el caso del "skimming" que es la implementación de un dispositivo que altera el funcionamiento normal de un cajero automático.

Coincidiendo con (Cano, 2009), se debe trabajar con énfasis en cuanto al fortalecimiento de las habilidades de administración de justicia, y su relación con los nuevos mecanismos de fraude y delincuencia informática:

1. Crear conciencia a los usuarios y público en general
2. Recolección constante de estadísticas y datos sobre incidentes informáticos
3. Capacitación continua al personal implicado en la seguridad
4. Asistencia en sitio para las unidades de lucha contra el delito informático
5. Actualización del marco normativo
6. Cooperación con los proveedores de alta tecnología
7. Investigaciones y publicaciones especializadas en crímenes de alta tecnología

8. Uso de herramientas forenses y de investigación criminal informática
9. Concienciación y compromiso de la gerencia
10. Estructuración de unidades de lucha contra el delito informático

Es así que, si se analiza lo estudiado en capítulos anteriores, las metodologías buscan de cierta manera, cumplir con al menos uno de los requerimientos listados, que habilitan el fortalecimiento de actividades contra el fraude y la delincuencia informática, que al final impacta sobre la información.

Marco legal Internacional

Según a un artículo escrito por (Borghello, 2009), en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la factibilidad de aplicar y armonizar en el plano internacional, las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales, mientras que en el año 1992, en el ocaso del siglo XX, la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburg (Alemania), adoptó múltiples recomendaciones con respecto a los delitos informáticos; entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá fomentarse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no es suficiente con la adopción de otro tipo de medidas como por ejemplo el "principio de subsidiariedad", es decir, que un asunto debe ser tratado por la autoridad más próxima al objeto del problema.

Cuarta Enmienda

Citando a la Constitución de los Estados Unidos de Norteamérica, la Cuarta Enmienda parte de la idea de que “la casa de cada hombre es su castillo” (Cornell University Law School, 2016), a salvo de averiguaciones y aprehensiones arbitrarias de propiedad por parte del gobierno. Protege contra las detenciones arbitrarias, y es la base de la ley con respecto a órdenes de registro, detener y registrar, inspecciones de seguridad, escuchas telefónicas y

otras formas de vigilancia, además de ser fundamental para muchos otros temas de derecho penal y de la ley de privacidad.

Textualmente, la Cuarta Enmienda de la Constitución de los Estados Unidos de Norteamérica dice que "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos, contra registros y detenciones arbitrarias, será inviolable, y no será emitida, a menos que sea por debido motivo, apoyado bajo juramento o protesta, y describan con particularidad el lugar para ser registrado y las personas o cosas que hay que serán intervenidas." (Cornell University Law School, 2016).

De esta Enmienda, se puede resumir que la información de una persona o institución deberán encontrarse a salvo contra registros arbitrarios, generalmente realizados por actividades de hacktivismo, de ciberdelincuencia, ingeniería social y/o ciberterrorismo. Debido a esto, una metodología de gestión de riesgo deberá partir de esta premisa con el objetivo de garantizar la confidencialidad e integridad de la información.

GLBA

La Ley Gramm-Leach-Bliley (GLBA o Ley GLB), también conocida como la Ley de Modernización Financiera del año 1999, es una ley federal aprobada en los Estados Unidos para controlar las formas en que las instituciones financieras hacer frente a la información privada de los individuos. La Ley consta de tres secciones: La Regla de Privacidad Financiera, que regula la recolección y divulgación de información financiera privada; Regla de las salvaguardias, que estipula que las instituciones financieras deben implementar programas de seguridad para proteger dicha información; y las disposiciones pretextos, que prohíben la práctica de pretextos (acceso a la información privada utilizando de manera fraudulenta). La ley también requiere que las instituciones financieras para dar a los clientes avisos de privacidad escritas que explican sus prácticas de intercambio de información.

HIPAA

Según un artículo de la Southern University, el estándar *Health Insurance Portability and Accountability Act* es una ley que busca el asegurar y proteger los registros médicos y otra información de salud personal. La regla define:

- Identificar un individuo y
- La custodia o intercambio electrónico o en copia física.

Si la información tiene componentes que deberían ser usados para identificar a una persona, esta debería ser protegida. La protección debe mantener con la información durante el plazo que la misma se mantenga alojada en la institución o en negocios asociados. La protección aplica a que la misma sea identificada individualmente en cualquier forma, ya sea electrónica o no electrónica, y en comunicaciones verbales, también deberían ser cubiertas.

Marco legal de la República del Ecuador

La Ley Orgánica de protección de datos personales.

Basado en el artículo 66 de la Constitución de la República del Ecuador, en la que establece que *"...Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley*", el Dr. José García define como datos personales a las "*informaciones, que permiten directa o indirectamente, identificar a la persona física a que se refiere, con independencia de que su procesamiento haya sido realizado por una persona física moral; o sea que son aquellos datos, con la suficiente fuerza individualizante, como para poder revelar aspectos de una determinada persona.*", es decir, información que hace referencia a cualquier dato de una persona, como puede ser el nombre, la edad, el sexo, etc. (García Falconí, 2011).

El Dr. García asegura que los datos personales deben ser correctos, completos, actualizados y relevantes, para la actividad en la cual serán utilizados, y, citando a F. Hindious, asegura que la protección de datos es "*Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular del derecho individual a la intimidad respecto del procesamiento manual o autónomo de datos*". Por otro lado, García citando a Antonio Pérez, define que la protección de datos es "el conjunto de bienes e intereses que pueden ser afectados por la elaboración de informaciones referente a las personas identificadas o identificables" (García Falconí, 2011).

El banco de datos, según García, "*es un conjunto de archivos interrelacionados, que es creado y manejado por un sistema de gestión o de administración de la base de datos; y, cualquier conjunto de datos almacenados electrónicamente o de manera manual*".

García Falconí, citando a Carlos Alberto Villalba señala que "Los bancos de datos son depósitos electrónicos de datos y de información. Esto implica una organización, un sistema de manejo de base de datos, un control que permite a los usuarios ingresar al

mismo de acuerdo a sus derechos de acceso, una administración o manejo de datos; un diseño de la base de datos y de su estructura, así como la selección e implementación de software que permite operarlo". (García Falconí, 2011)

Los datos, según García, de forma legal son reconocidos bajo la siguiente clasificación:

a) Personales; que incluyen características relacionadas al estado civil, trabajo, registros escolares y estudiantiles, bancarios, de mandato, policiales, militares, etc.;

b) Comerciales; que pueden ser: libros de accionistas, societarios, los balances, etc.;

c) Impositivos; que en otras palabras hace referencia a los registros de comercio;

d) De propiedad; relacionado a los bienes que poseen las personas, naturales o jurídicas;

e) Políticos; relacionado con las creencias en esta materia; y,

f) Sanitarios; esto es referente a la salud personal.

La doctrina indica que los registros, archivos, bases de datos, no necesariamente deben ser informáticos o automatizados, pues debe contemplarse como información cualquier registro, ya sea electrónico o no. Además, menciona que los registros deben ser accedidos solamente por personas o sistemas autorizados, y que cada uno de los sujetos mencionados deben mantener responsabilidad sobre su interpretación y uso.

La Constitución de la República en el Art. 66 numeral 19 garantiza la protección de datos de carácter personal. Para defender este derecho, se cuenta con la garantía del **hábeas data**, la misma que está regulada en el Art. 92 de dicha Carta, la cual dispone que "*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos".*

García menciona que las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada solamente con autorización de su titular o de la ley.

Además, menciona que "la persona titular de los datos, podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados". (García Falconí, 2011)

Concluye García que, es necesario y fundamental emplear una reforma constitucional que señale "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". (García Falconí, 2011).

(Páez Rivadeneira, 2010), indica que lo que establece el artículo 23 de la Ley Orgánica de Protección de datos, referido a la interconexión entre datos públicos y privados, rompe todo principio ético, y que atenta la privacidad y la intimidad de los datos de las personas, ya que puede ser mal empleado por los funcionarios públicos que manejen el sistema. Así también menciona que los legisladores deben proteger los derechos de los ciudadanos, mas no dar herramientas que conlleven a la persecución política o al funcionamiento de la represión y la violación de los Derechos Humanos.

Por otro lado, el Superintendente de Telecomunicaciones del Ecuador en el año 2014, Fabián Jaramillo Palacios, mencionó que en Ecuador se había optado por la protección de la información personal a través del Habeas Data, con algunos inconvenientes. Entre ellos menciona a la escasa protección de la información, que es de tipo judicial, donde el reclamo es ex post y que no tiene un sentido preventivo (Jaramillo Palacios, 2014).

Páez coincide con García en que la protección de datos debería enfocarse a proteger a una persona ante el manejo o manipulación no autorizada de sus datos personales; además de que los resultados de los procesamientos informáticos deberían ser identificables con el titular de los mismos, y el consentimiento no autorizado del uso de datos.

Ley Orgánica de transparencia y acceso a la información pública

Esta Ley, según (Jaramillo Palacios, 2014), garantiza el derecho de acceder a las fuentes de información, además de ser un mecanismo para ejercer la participación democrática respecto del manejo de la cosa pública y la redición de cuentas, y que la información confidencial está excluida del principio de publicidad.

Asimismo, indica que el Art. 6 de la Ley de Transparencia y acceso a la información Pública, utiliza una redacción inadecuada cuando define la información confidencial como: "aquella información pública personal…", debido a que los datos personales no pueden ser considerados como información pública.

Jaramillo menciona además sobre la creación de la Ley del Sistema Nacional de Registro de Datos Públicos - SINARDAP, cuya finalidad es proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la Ley y en normas de registros; con el objeto de coordinar el intercambio de información de los registros de datos públicos, y también menciona que en caso que las entidades privadas posean información de naturaleza pública, también serán incorporadas a este sistema.

Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, el comercio electrónico y la protección a los usuarios y datos de estos sistemas (Jaramillo Palacios, 2014).

Ley de comercio electrónico

En cuanto a la ley de comercio electrónico – Art. 9: Protección de datos, (Jaramillo Palacios, 2014) hace referencia a que, "*para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de estos, quien podrá seleccionar la información a compartirse con terceros. Además, la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad*

garantizados por la Constitución de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular, u orden de la autoridad competente."

Junta Bancaria

La (Superintendencia de Bancos y Seguros, 2012), en la resolución JB-2012-2148, establece que

"39.2 Protección contra clonación de tarjetas.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;"

En cuanto a control de riesgos, la SIB define en la misma resolución que:

"2.35 Calidad de la información. - Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella; "

"2.37 Confiabilidad. - Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones; "

"4.3.8.2 Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información"

"4.3.8.7 Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas"

Claramente se puede validar que esta resolución obliga a las instituciones financieras a incorporar mecanismos que protejan la información confidencial de los clientes, que muchas veces es accedida por el personal de desarrollo de sistemas, elevando el riesgo de manipulación o hurto de la misma.

Aspectos relevantes relacionados a la trazabilidad, se pueden validar por ejemplo en la siguiente disposición:

"4.3.8.8 Ofrecer a los clientes los mecanismos… Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros…"

Donde se requiere dejar un registro de las cuentas, de las direcciones IP, o de los números autorizados, además de los montos máximos; es decir, dejar rastro de lo que se ha producido durante un proceso determinado.

Disposiciones como *"4.3.8.13 Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas"* sugieren que debe existir un marco de regulaciones institucionales que aseguren los procesos relacionados con la administración, transporte, instalaciones y mantenimiento, no solo de los canales electrónicos, sino de cualquier elemento que sea portador de información.

"4.3.8.16 Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. "

Además, menciona que "*todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos "*, elemento clave a contemplar en una metodología que sugiere la implementación de contramedidas para la mitigación de riesgo, en este caso, políticas y procedimientos de seguridad de la información.

"4.3.8.24 Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad;"

Según esta disposición, la metodología a desarrollar debería considerar aspectos que permitan a las entidades de control, evaluar los procedimientos y actividades contempladas en la misma; o bien, estar alineada a una metodología internacional como COBIT, que, entre uno de sus dominios, permite lograr este objetivo.

Conclusiones del capítulo 4

El objeto de la Ley consiste en garantizar los derechos Constitucionales, que, según Jaramillo, hacen referencia al Derecho a la privacidad y el Derecho a la protección de datos personales. La Ley mantiene los siguientes principios:

Legalidad, condición o acto realizado dentro del marco normativo, es decir, que debe realizarse de acuerdo a la Ley vigente y su jurisdicción, y no a la voluntad de las personas;

Finalidad porque contribuye al logro del bien común de las personas que forman parte de una sociedad

Libertad, debido a que la Ley implica en reconocer en cada persona su igualdad en el derecho a la libertad. Al formar parte de una sociedad independiente, algunas limitaciones a la libertad son esenciales para evitar otras restricciones de mayor incidencia (Merma Aroni, 2002).

Calidad de los textos normativos, ya que las Leyes deben estar correctamente conformadas, deben ser claras y no ser anticonstitucionales. La Constitución de la República de Colombia menciona que el principio de Calidad consiste en que *"toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad."* (Presidencia de Colombia, 2014)

Consentimiento: en los casos en los que se requiere el consentimiento de una persona para el tratamiento de sus datos personales, esto es, a elegir el nivel de protección que cada persona quiere dar a la información a ella referida.

Transparencia: *"Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley"* (Presidencia de Colombia, 2014).

Acceso y circulación restringida, hace referencia a que *"el derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de promover y generar una*

cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros".

La información para cualquier institución o persona natural son esenciales. Las metodologías estudiadas en los capítulos anteriores, entre otras cosas, se basan en función a un marco legal. De lo revisado en este capítulo, Ecuador aún no tiene leyes claras en cuanto a la confidencialidad de la información, sin embargo, se sabe que son aspectos que deben ser considerados en una metodología, a manera de que esta sea un referente empresarial para la protección de información.

Finalmente, se puede argumentar, que, de todos los mecanismos listados al inicio de este capítulo, se podría decir que, es vital que, para las MPYMES, el marco legal organizacional considere, al menos, los siguientes elementos:

- Concienciación a los usuarios y público en general
- Recolección constante de estadísticas y datos sobre incidentes informáticos (recopilación de los incidentes en bitácoras de control)
- Capacitación continua al personal implicado en la seguridad de la información.
- Actualización del marco normativo, es decir, del documento que contiene las políticas de seguridad de la información.
- Concienciación y compromiso de la gerencia, pues la única forma de que un sistema de gestión de seguridad de la información funcione, es cuando la alta dirección o la gerencia general respaldan los compromisos relacionados con el uso de los recursos de información.

Este marco legal es el que establecerá y regulará las actividades a considerar para que la metodología a desarrollar permita verdaderamente cumplir con su objetivo: la mitigación del riesgo.

Capítulo 5: Estado actual de las MPYMES en cuanto al riesgo de información

"A pesar de que se han hecho esfuerzos, en Ecuador, todavía no se trabaja en seguridad de manera sistemática con políticas definidas. El Gobierno no tiene un plan de acciones para todas las entidades del país. Muchas veces es el propietario o el administrador del sitio web el que decide qué hacer para que este sea seguro, por ello Ecuador llega a ser un blanco fácil de los atacantes. Ecuador es un blanco fácil para ataques de hackers" (Dimitry Bestuzhev, 2011).

En la experiencia profesional mantenida a lo largo de múltiples observaciones, entrevistas con gerentes, usuarios, técnicos informáticos; además de constantes actividades de consultoría; ha motivado en primera instancia a comparar cada institución, organización y empresa de diferente ámbito, con un solo propósito: El de establecer el grado de madurez de las PYMES en cuanto a la gestión de riesgo.

Para determinar la situación de las empresas frente al riesgo, se ha empleado el método no probabilístico de muestreo por conveniencia, que se trata de una técnica comúnmente usada en la que se selecciona una muestra de una población que accesible, es decir, que se seleccionan porque están fácilmente disponibles y no necesariamente haber sido seleccionados bajo un criterio estadístico; lo que posibilita la generalización a sujetos similares (Bernal, 2006).

Para la muestra por conveniencia se han tomado como criterio principal, la localidad, la capacidad de gestión, tamaño e importancia de la unidad productiva y la significación de su magnitud de riesgos en términos de importancia y magnitud de operaciones (Bernal, 2006).

De acuerdo a diferentes opiniones y jurisprudencia de hechos y procesos de varios investigadores, no se debe considerar el muestreo por conveniencia como un método inútil, ya que por lo manifestado es habitual su uso exitoso en muchos ámbitos (Garcés, 2000).

Como parte fundamental de este proceso se utilizó el muestreo por cuotas, técnica utilizada en investigación mediante paneles, considerando que constituye la versión no probabilística del muestreo estratificado. De esta manera, de acuerdo con Ochoa (2015), se han considerado las siguientes etapas:

1. Primeramente, se han tomado las estadísticas disponibles del INEC, SRI, y de entidades relacionadas para obtener el universo total, con lo cual se ha dividido la población objeto de estudio en grupos de forma exhaustiva (todos los individuos están en un grupo) y mutuamente exclusiva (un individuo sólo puede estar en un grupo), de manera parecida a la división en estratos empleada en el muestreo estratificado. Esta segmentación se la realizó considerando al tamaño de la empresa y los niveles de riesgo como variables sociodemográficas (Ochoa, 2015).

2. Consecuentemente, se ha considerado el objetivo y el objeto de estudio, con la finalidad de definir los procesos de toma de datos y procesamiento de la información para cada uno de estos grupos. Para ello, se han considerado estos objetivos de forma proporcional al tamaño del grupo en la población, los mismos que se conocen como cuotas, considerando la posibilidad de ocasionalmente definir cuotas no proporcionales a la población, lo que ha permitido profundizar en el análisis de un grupo específico (Ochoa, 2015).

3. Por último, se seleccionaron participantes (fuentes de información) y un modelo de comprobación para cubrir cada una de las cuotas definidas. Este es el punto en el que se distancia este modelo del muestreo probabilístico; ya que en el muestreo por cuotas se acepta que la selección de individuos no sea aleatoria, pudiendo ser una selección mediante muestreo por conveniencia (Ochoa, 2015).

La diferencia entre el muestreo estratificado y el muestreo por cuotas está en la forma en la que se han seleccionado los participantes. En el muestreo estratificado se dispone de una lista de posibles unidades de muestra, todas ellas con una cierta probabilidad (conocida) de ser seleccionadas. En el muestreo por cuotas no; pues se requiere de elementos muestrales

obtenidos de forma no aleatoria, por lo que se tiene que seguir un proceso de comprobación y validación antes de tomar la información de campo, considerando si son o no válidos para el estudio (es decir, si puede formar parte de una de las cuotas o si ya he excedido el objetivo), hablamos de un individuo descartado por ser **quota-full** (Ochoa, 2015).

El uso de cuotas en un muestreo no probabilístico no permitirá transformarlo en probabilístico. Así se seguirá sin poder calcular el margen de error y el nivel de confianza sobre los resultados. Es decir, el uso de cuotas no permite medir el grado de precisión de los resultados a obtener.

Por el objeto de estudio y por considerar que esta es una propuesta piloto, se considera que es válido a efectos de tener una idea significativa de la problemática, ya que es una propuesta general sobre un proceso de mejora de procedimientos y normativas ya existentes, vigentes y validadas, puesto que usar cuotas es un sistema efectivo y económico de obtener muestras que proporcionan información relevante.

Se puede decir entonces que, el muestreo por conveniencia es una técnica de levantamiento y obtención de información no probabilístico donde los sujetos son seleccionados en base a criterios profesionales y técnicos relacionados con la investigación y la posibilidad de obtener un criterio valido en un proyecto o propuesta piloto de investigación.

Para obtener esta proporción, se ha requerido estimarla en base a las siguientes consideraciones:

1. El total de la población, según el INEC (2015), el sector económico está clasificado de acuerdo a las siguientes actividades económicas:

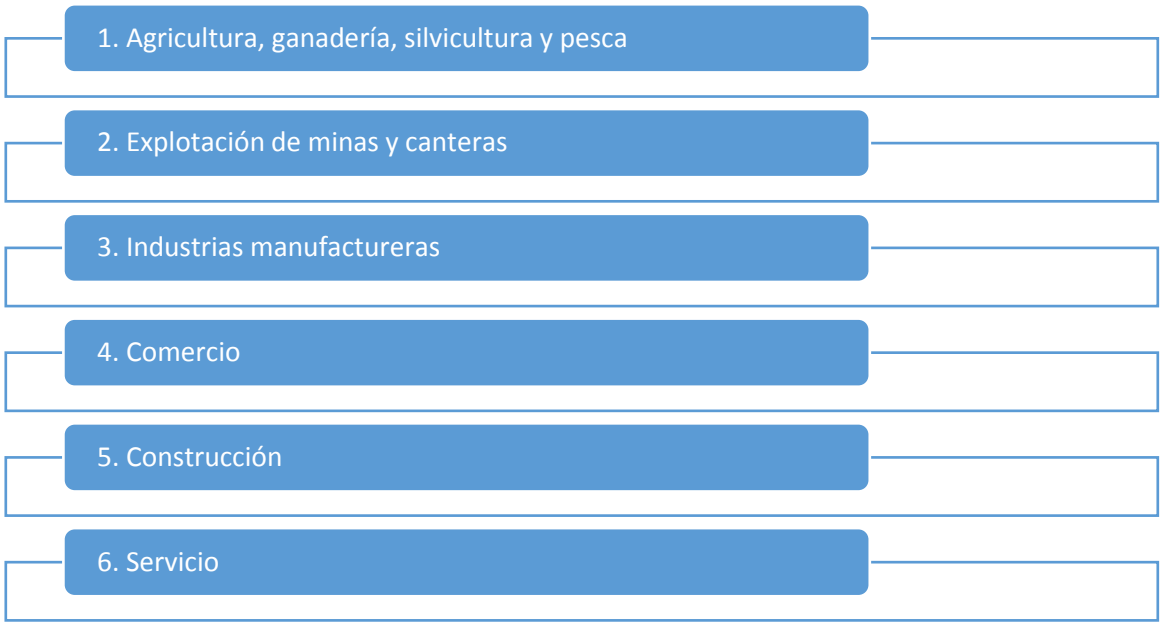


Ilustración 3: Actividades económicas según el INEC 2015. Fuente: INEC, 2015

2. Para la estratificación de selección inicial, se ha considerado las estadísticas del INEC (2015), donde se menciona que para el 2014, 843.644 empresas registraron alguna de las actividades económicas en base a una de las siguientes condiciones: 1) Ventas declaradas al SRI, 2) Personal afiliado al IESS y 3) Perteneciendo al RISE, han declarado sus impuestos al SRI. De las 843.644 empresas se descartan directamente a las 4.253 empresas que forman parte de las grandes organizaciones, quedando así un universo de 839.391 empresas del sector MPYME.

3. Del total de empresas mencionado anteriormente, el 43.6% son Microempresas, pertenecientes al RISE (INEC, 2015), presentando ingresos inferiores a 60.000 USD.

4. Únicamente 362.083 de las empresas registran información de personal afiliado (INEC, 2015)

5. 66.551 empresas cuentan con información de declaración de ventas al SRI y personal afiliado (INEC,2015)

6. Del total de 66.551 empresas, se ha medido una proporción del 5%, con una precisión del 6% y un nivel de confianza del 95%, lo que da un total de 50 empresas, luego de aplicar la siguiente ecuación de estimación de proporción.

Se calcula el nivel de riesgo en base a un estudio de tipo social, en el que se considera:

- Importancia relativa
- Impacto relativo
- Peso específico (importancia que tiene la muestra del total de empresas de riesgo)
- Condiciones socioeconómicas como: capacidad de inversión, ingreso y capacidad de operación. Esto es, la cantidad de recursos que requiere el departamento de TI para gestionar la información.
- Al ser un proyecto piloto, por lo tanto, se utiliza un nivel de error determinado, que consecuentemente concluye en un estudio no probabilístico por conveniencia.

Esto concluyó en un estudio descriptivo a 50 empresas del sector MPYME a nivel nacional, debido a conveniencia por aspectos de consultoría que desarrolla el autor de este trabajo. La distribución de las mismas se presenta en la tabla a continuación.

Tabla 7: Distribución de las empresas a evaluar.

Industria	Número de empresas
Salud	4
Comercio	9
ONG	4
Gobierno	9
Finanzas	4
Software	3
Educación	1
Hardware	2
Consultoría	5
Automotriz	3
Hotelería/Restaurantes	2

Diseño	1
Comunicación	2
Joyería	1
TOTAL	50

Fuente: Autoría Propia

La siguiente gráfica resume la tabla anterior, indicando el porcentaje de la muestra obtenida por estas empresas, organizaciones e instituciones estudiadas.

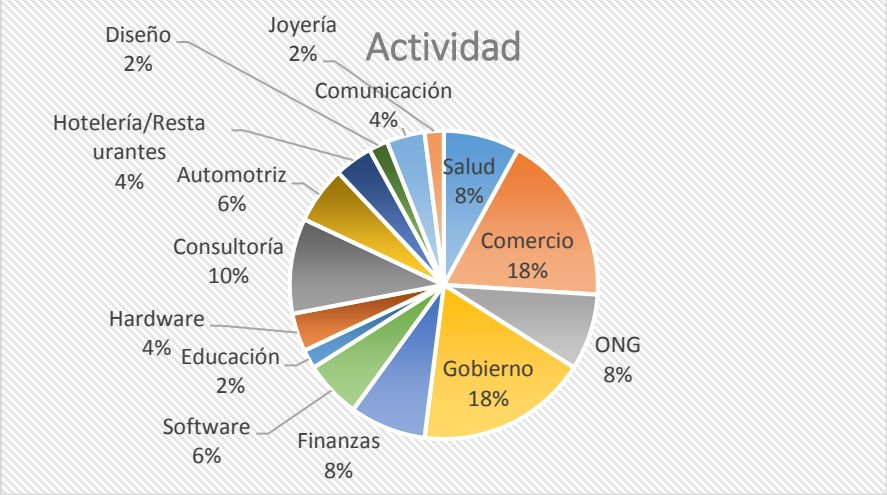


Ilustración 4: Actividad a la que se dedican las empresas estudiadas. Desarrollado por: El Autor

Una de las preguntas realizadas durante la entrevista fue si las empresas han identificado los activos de información, comprendiendo que estas hacen referencia al hardware, software, información electrónica, información en papel, recursos humanos, comunicaciones, proveedores de servicio y elementos de respaldo. La respuesta, se ve reflejada en la siguiente gráfica:

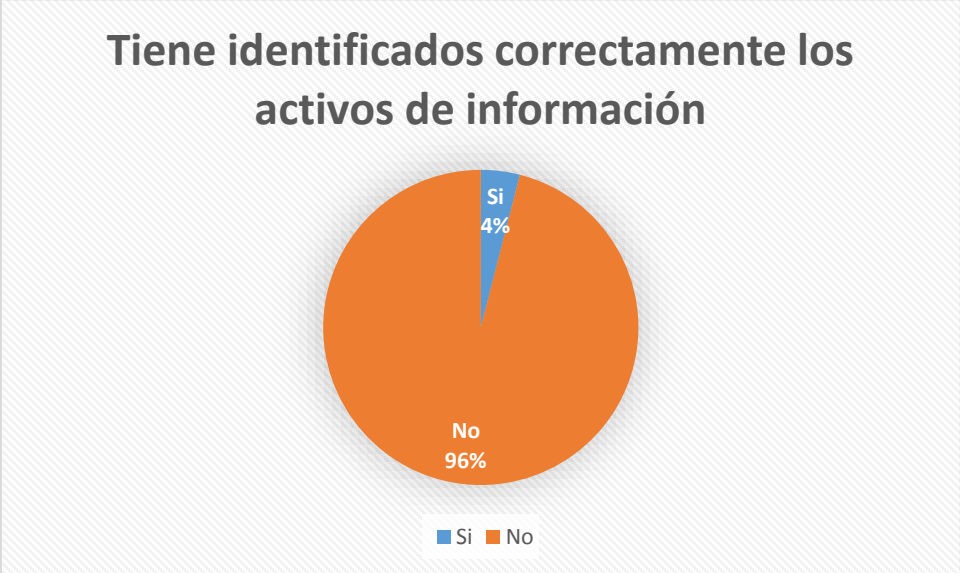


Ilustración 5: Identificación de los activos de información. Fuente: Estudio realizado por el Autor

Esto resume que solo un 4% de las empresas del sector MPYME ecuatorianas analizadas no cuentan con una identificación de sus activos de información, recalcando que la primera vez consideraron erróneamente como activo a los elementos que forman parte del registro contable.

Del escaso 4% mencionado anteriormente, solo el 2% mantiene actualizado el inventario de los activos de información, tal como se lo puede apreciar en la figura a continuación.

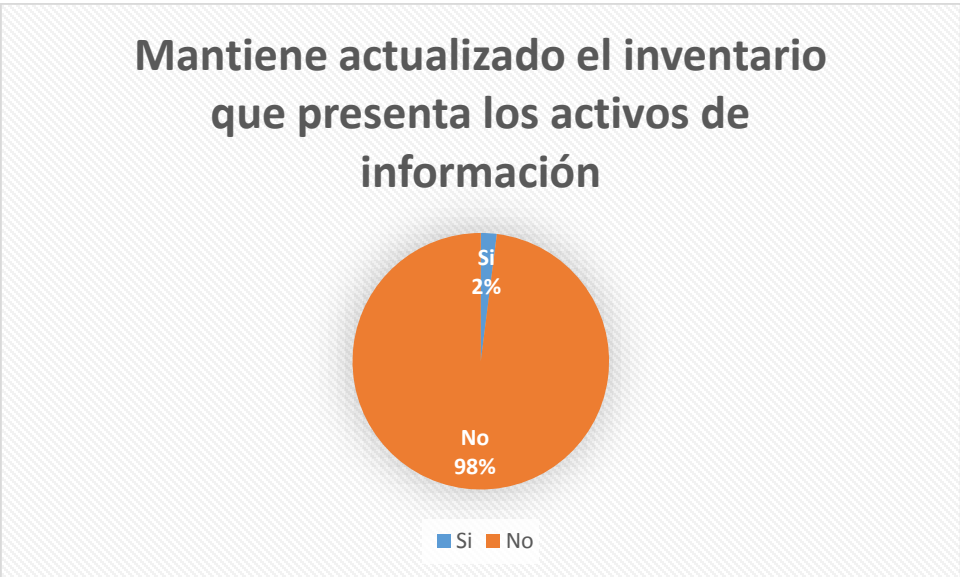


Ilustración 6: Actualización del inventario de activos de información. Fuente: Estudio realizado por el autor

A manera de conocer las actividades elementales para gestionar el riesgo de información, se mantuvo la siguiente pregunta: ¿Realiza usted respaldos de la información? El 100% aseguró realizar la mencionada actividad.

Ilustración 7: Realiza respaldos. Fuente: Estudio realizado por el autor

Sin embargo, esas actividades no son del todo formales. Así se pudo constatar que solo un 42% los realiza mediante procedimientos establecidos de manera formal en la institución, muchas veces solicitados por las instituciones de control.

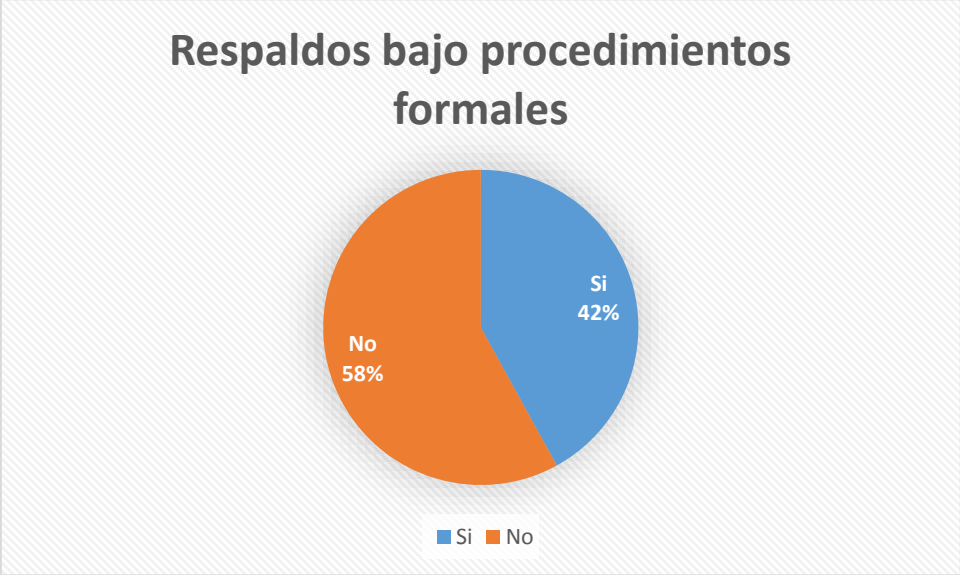


Ilustración 8: Realiza respaldos bajo procedimientos formales. Fuente: Estudio realizado por el autor.

Solamente un 24% de las instituciones tienen delimitadas las áreas físicas sensibles del negocio, haciendo que, para el resto de las instituciones, las áreas físicas, a pesar de ser identificadas, no son del conocimiento de los usuarios internos y externos, quedando un inminente riesgo sobre la información que se maneja en cada una de esas áreas.

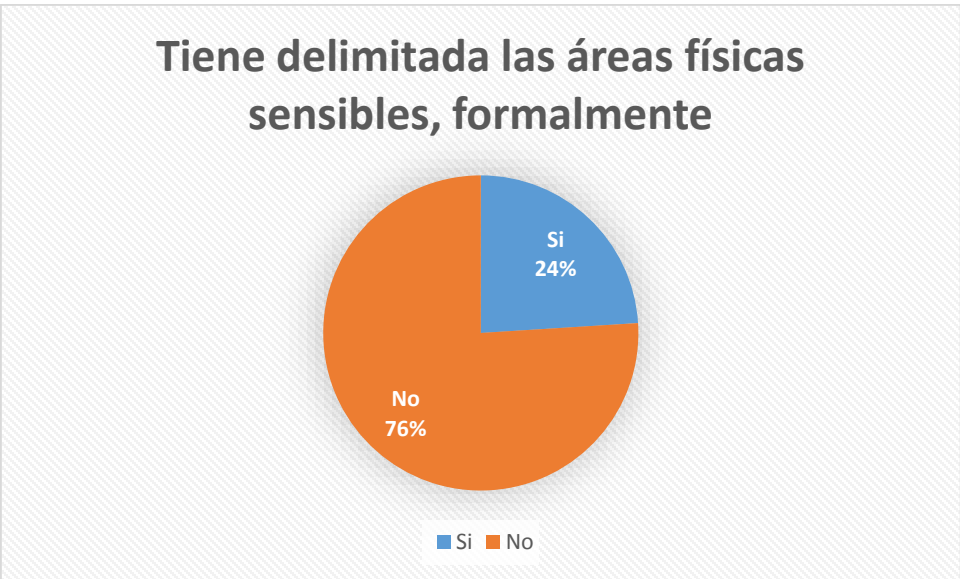


Ilustración 9: Delimitación formal de las áreas físicas sensibles. Fuente: Estudio realizado por el autor

En cuanto a planes para protección de los recursos humanos, se puede evidenciar que no existen procedimientos formales para llevar a cabo la evacuación de un edificio en caso de un incidente. Así, solamente un 14% de los entrevistados saben, formalmente, que hacer.

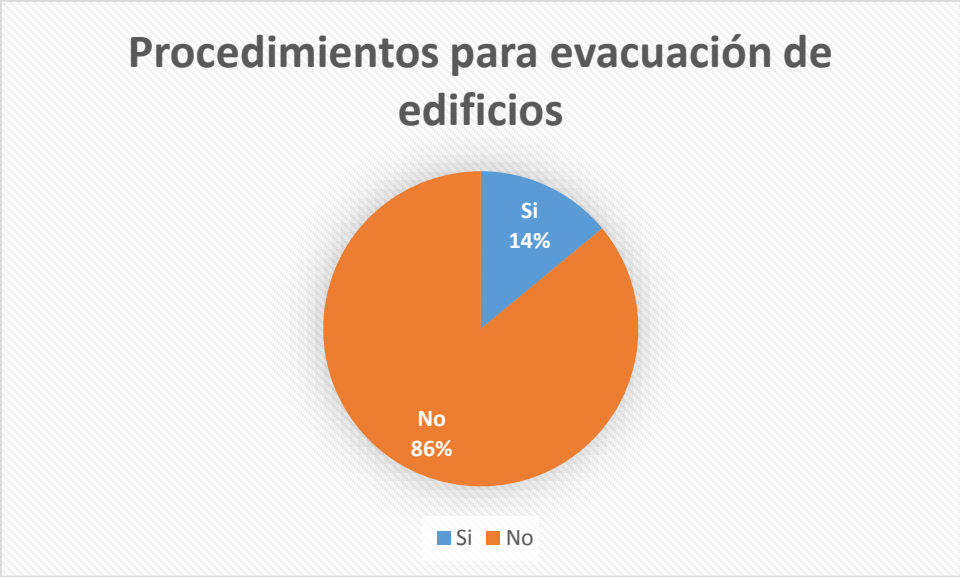


Ilustración 10: Procedimientos para evacuación de edificios. Fuente: Estudio realizado por el autor.

Este tipo de actividades sugiere, por ejemplo, identificar rutas de escape, puntos de concentración, bitácoras de seguimiento, procedimientos para simulacros, entre otras que son críticas para salvaguardar al recurso humano y la información sensible en papel. Para este último, muchas veces se sugiere hacer el procedimiento de la "cajita feliz", que consiste en ubicar la información crítica en uno de los cajones del escritorio, y que, en caso de incidente, el empleado esté en la capacidad de tomar esta caja o cajón y llevarlo consigo durante el proceso de evacuación.

En cuanto a las amenazas, se puede comprobar que solo el 16% de las instituciones analizadas tienen un registro formal de las amenazas que pueden presentarse en el entorno empresarial, ya sean estas físicas o lógicas. La gráfica a continuación resume los resultados.

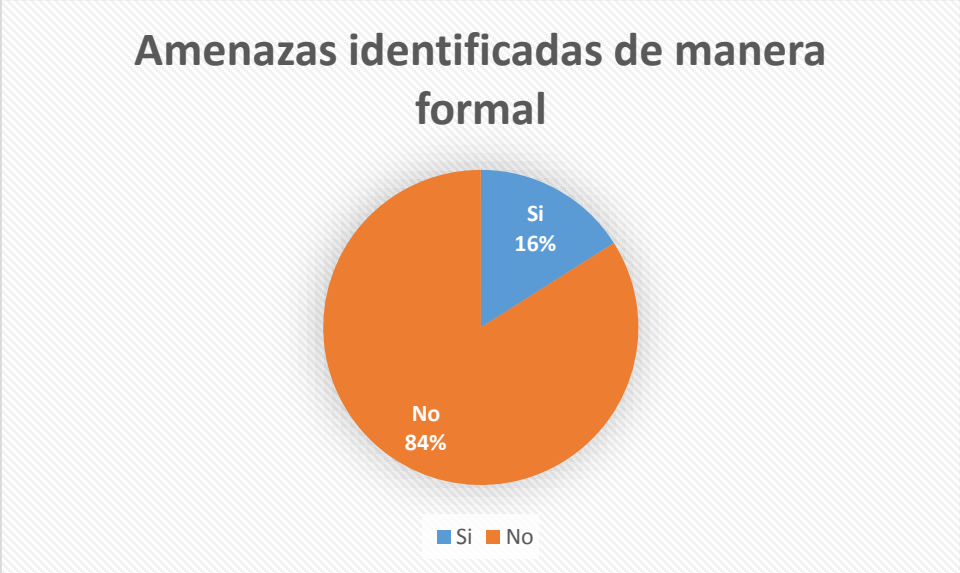


Ilustración 11: Amenazas identificadas de manera formal. Fuente: Estudio realizado por el autor.

En la siguiente gráfica se puede comprobar que, únicamente el 2% de las empresas analizadas cuentan con planes formales para la gestión de riesgo de la información, de las cuales, dentro de la práctica se han basado en la metodología Magerit para alcanzar tal fin.

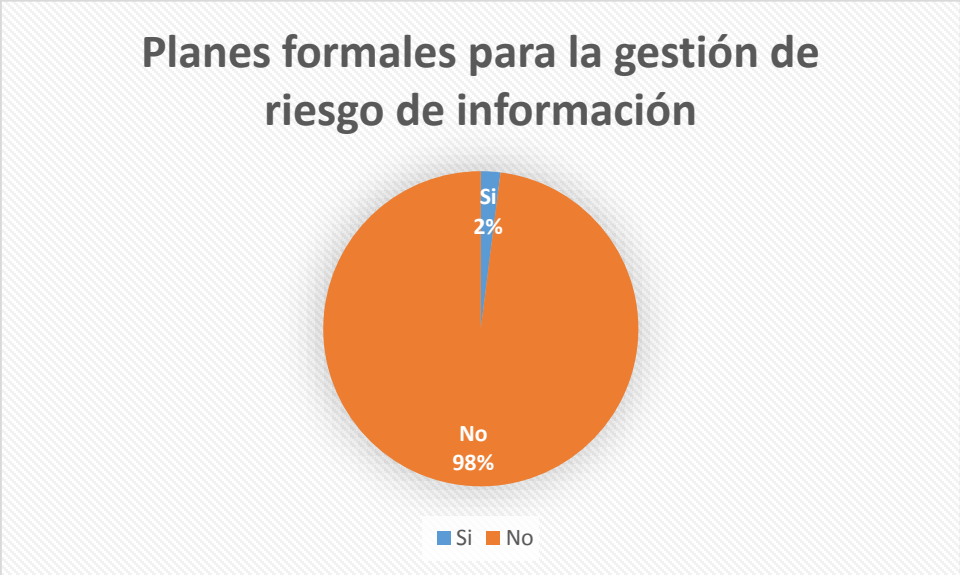


Ilustración 12: Planes formales para la gestión de riesgo de información. Fuente: Estudio realizado por el autor.

Finalmente se ha podido comprobar que las razones por las que las empresas que no cuentan con un plan de gestión de riesgo formal, se resume en el desconocimiento del

proceso de gestión de riesgos, en la falta de presupuesto, y en la complejidad que presentan las normas ISO. La gráfica a continuación resume esta afirmación.

Ilustración 13: Razones por las que las empresas no han adoptado un plan de gestión de riesgos formal. Fuente: Estudio realizado por el autor.

Conclusiones del capítulo

Luego de haber realizado una entrevista a los responsables de la gestión de las empresas del sector MPYME, de diferentes actividades económicas, se ha podido ver que el nivel de madurez en cuanto a gestión de riesgos es solo por iniciativa, o prácticamente es nula.

Los incidentes producidos en Ecuador tras el terremoto del 16 de abril del 2016 han revelado que no solo las empresas están inmersas en el riesgo y que no tienen claros planes de contingencia, sino que toda una población no tiene actividades definidas ante la materialización de una amenaza. Comparando el Ecuador con países como Chile o Japón, aún hay mucho trabajo por realizar, en donde es imprescindible concienciar a la población y mantenerla preparada ante incidentes.

Por otro lado, de acuerdo con el comentario de Bestuzhev, el Ecuador mantiene un alto nivel de riesgo en cuanto a información se trata. La iniciativa tomada por el administrador de la página web, o del técnico de soporte institucional no es suficiente, es por ello que el

alto mando de cualquier institución, ya sea pública, privada o sin fines de lucro, deben estar conscientes de los graves problemas que puede acarrear su organización cuando la amenaza se materializa.

Los resultados de la entrevista han podido revelar que, por ejemplo, si bien se realizan copias de seguridad de la información mantenida en los servidores de la empresa, estas actividades no son formales, no cuentan con evidencia de hacerlas de forma periódica y, peor aún, las copias nunca han sido probadas.

De esta manera, se puede afirmar que las empresas del sector MPYME, cuya definición fue realizada en el capítulo 1 de este documento, no cuentan con una metodología clara de actividades que deberán realizar para la gestión de los activos de información y los riesgos que pudiesen presentarse.

Capítulo 6: Proyección hacia COBIT 5 y COSO III

Introducción

Hoy en día, los marcos de gestión empresariales más utilizados en las grandes empresas posiblemente son COBIT y COSO. Toda empresa, por más pequeña que sea, busca la competitividad, que para (Minchala, 2016), es lograda mediante el fortalecimiento en la gestión de sus procesos administrativos, organizando y gestionando de manera adecuada sus recursos.

En su trabajo de grado, (Minchala, 2016) asegura que tanto COBIT 5 como COSO III, se encuentran alineadas a las normativas ISO 27001, 27002, 27005 y 31000.

La siguiente sección plantea revisar brevemente los aspectos clave que deberá considerar la metodología a proponer a manera de que pueda proyectarse a ser un elemento que

contribuya a la gestión de gestión de riesgos que tanto COBIT como COSO tienen como objetivos.

COBIT 5

Para (Minchala, 2016), "*COBIT 5 – es una nueva versión del ya conocido estándar para el cumplimiento de objetivos de control para el CIO (Chief Information Officer - Oficial en Jefatura de Sistemas) y su área*", versión que proporciona un marco de referencia integral, el mismo que contribuye alcanzar los objetivos corporativos mediante un adecuado y efectivo gobierno de TI.

Menciona (Minchala, 2016), que COBIT 5 hace posible que las Tecnologías de Información en una organización sean gobernadas y gestionadas en forma holística, considerando a toda la organización y sus áreas funcionales, así como los interesados internos y externos.

COBIT está conformado por 7 habilitadores de gestión, conocidos también como catalizadores corporativos:

- Principios, políticas y modelos de referencia
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Gente, habilidades y competencias. (Minchala, 2016)

De todas las metodologías que se utilizan para la gestión de riesgos, COBIT es la única que se preocupa de tomar los controles técnicos y acoplarlos a los requerimientos del negocio. Así, según Minchala, COBIT 5 se basa en ISO/IEC 15504 e ITIL.

Citando a (ISACA, 2012), (Minchala, 2016) aduce que el riesgo de TI es *"un riesgo para el negocio, específicamente el riesgo para el negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI dentro de una empresa".*

De esta manera, se puede comprobar que uno de los objetivos que plantea COBIT es, obviamente, el de proporcionar controles que permitan gestionar el riesgo de TI.

COBIT se resume en 5 principios:

- Satisfacer las necesidades de las partes interesadas
- Cubrir la empresa de extremo a extremo
- Aplicar un marco de referencia único integrado
- Hacer posible un enfoque holístico
- Separar el gobierno de la gestión

La metodología a ser propuesta deberá incluir un análisis del contexto organizacional, en base a herramientas propias de las ciencias de la administración, en los que se analice el estilo de la empresa, los recursos humanos y sus habilidades, los procedimientos y políticas corporativas y los valores compartidos.
Las tecnologías de la información son transversales, es decir, apoyan en todos y cada uno de los procesos empresariales, por lo tanto, deben ser adecuadamente planificadas, implementadas, monitoreadas y gestionadas.

(Minchala, 2016) sugiere que las categorías de riesgo que se producen en el área de TI y que deben ser consideradas y analizadas son las siguientes:

Categorías de Riesgo TI

- Establecimiento y mantenimiento del Portfolio de Proyectos
- La Gestión del ciclo de vida de los Proyectos
- El Proceso decisorio de las inversiones de TI
- Experiencia y habilidades de los recursos de TI

- Operaciones del personal (Abusos e Intentos Maliciosos)
- Información (Filtraciones, Perdidas, Accesos Indebidos)
- Arquitectura de TI (Visión y Diseño)
- Infraestructura (Hardware, Software, Selección, Implementación y Baja de Sistemas)
- Software (Ciclo de Vida)
- Ineficaz pertenencia del negocio de TI (Compras Departamentales, Requerimientos inadecuados)
- Selección de Proveedores de TI
- Cumplimiento Regulatorio
- Geopolítica (Interferencia Gubernamental, Acciones dirigidas)
- Robo de Infraestructura
- Malware
- Ataques Lógicos (Espionaje Industrial, Virus)
- Acción Industrial (Huelgas, Paros directos o indirectos)
- Entorno (Equipamiento no amigable con el entorno)
- Actos de la naturaleza
- Innovación (Tendencias)

Así, (Minchala, 2016) citando a (Ritegno, 2012) menciona también que, en el ámbito de riesgos COBIT presenta dos perspectivas:

- **la función de riesgo**: La perspectiva de la función de riesgo se enfoca en lo necesario para construir y mantener la función de riesgo en la organización.

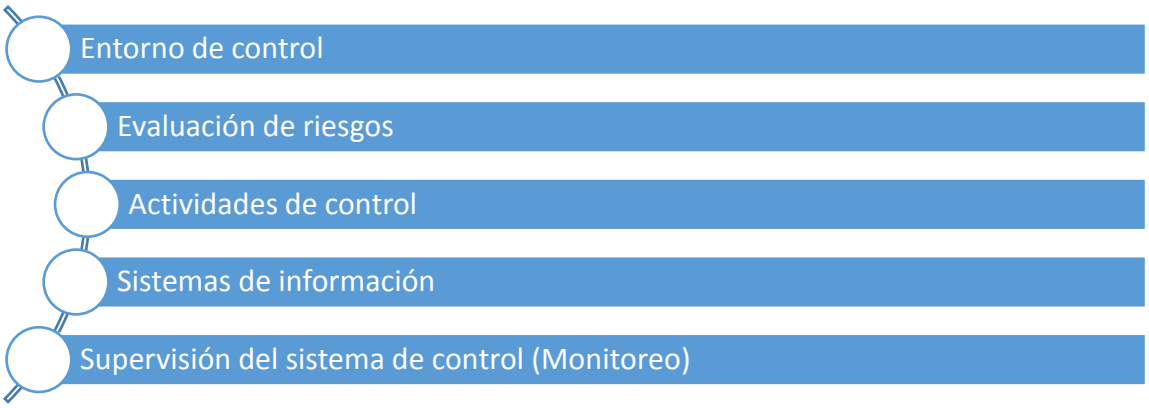
- **la gestión de riesgos:** La perspectiva de la gestión de riesgos se concentra en los procesos básicos de gobierno y gestión del riesgo con el objetivo de optimizar el riesgo y en los procedimientos para identificarlos, analizarlos, tratarlos y reportarlos diariamente.

COSO III

(Minchala, 2016), citando a (AUDITOOL, 2013), indica que: "*Las empresas deben implementar un sistema de control interno eficiente que les permita enfrentarse a los rápidos cambios del mundo de hoy, y permita enfrentar los riesgos. El marco integrado de control interno propuesto por COSO provee un enfoque integral y herramientas para la implementación de un sistema de control interno efectivo y en pro de mejora continua. Un sistema de control interno efectivo reduce a un nivel aceptable el riesgo de no alcanzar un objetivo de la entidad*".

COSO, Committee of Sponsoring Organizations of the Treadway Commission, está compuesto por 5 componentes y 17 principios, los mismos que establecen las mejores prácticas para llevar a cabo con control interno de la organización. (Minchala, 2016)

Los componentes que plantea COSO III son los siguientes:



Y sus principios pueden resumirse en los siguientes puntos:

Principio 1: La organización demuestra compromiso con la integridad y los valores éticos
Principio 2: El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.
Principio 3: Establece estructura, autoridad y responsabilidad

Principio 4: Demuestra compromiso para la competencia

Principio 5: Hace cumplir con la responsabilidad

Principio 6: Especifica objetivos relevantes

Principio 7: Identifica y analiza los riesgos

Principio 8: Evalúa el riesgo de fraude

Principio 9: Identifica y analiza cambios importantes

Principio 10: Selecciona y desarrolla actividades de control

Principio 11: Selecciona y desarrolla controles generales sobre tecnología

Principio 12: Se implementa a través de políticas y procedimientos

Principio 13: Usa información Relevante

Principio 14: Comunica internamente

Principio 15: Comunica externamente

Principio 16: Conduce evaluaciones continuas y/o independientes

Principio 17: Evalúa y comunica deficiencias

(Minchala, 2016) resume a COSO como "un marco integrado de control interno organizacional, que reúne las mejores prácticas para administrar de forma eficaz la empresa, asegurando el alcance de los objetivos propuestos; esta norma nace con el propósito de estandarización de normas y políticas del control interno de las instituciones".

Conclusiones del capítulo 6

Las metodologías de gestión de Riesgos COBIT 5 y COSO III tienen como base principal la organización, y contemplan el riesgo tecnológico como un impedimento para alcanzar los objetivos corporativos.

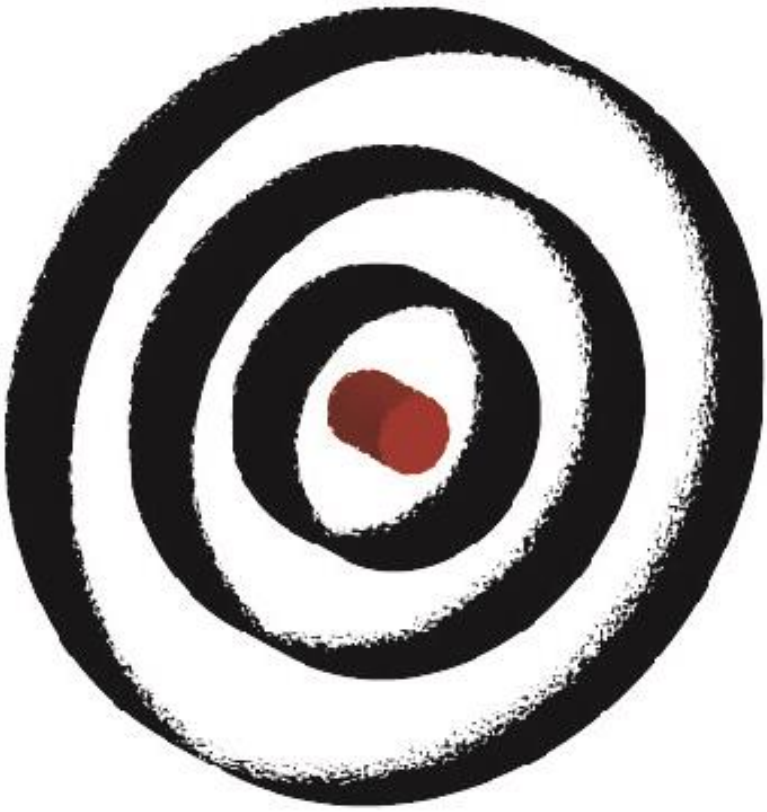
Así, de lo revisado en este capítulo, se puede argumentar que, para que la metodología a proponer tenga una proyección con COSO III, deberá incluir aspectos relacionados a:

- Identificación del contexto organizacional
- Evaluar aspectos que conlleven a fraudes

- Identificar actividades de control (Establecimiento de contramedidas)
- Monitoreo continuo y
- Reportar a los interesados.

Considerando a COBIT 5, la perspectiva de la metodología a proponer se enfocaría a la gestión de riesgos, ya que se partiría de los procesos básicos de gobierno y gestión del riesgo, contemplando procedimientos para cada una de las fases involucradas: identificación, análisis, tratamiento, monitoreo y reporte permanente.

COBIT proporciona un cuadro de interacciones que se producen entre el Gobierno y la Gestión, las mismas que deberían ser consideradas en el análisis del contexto que formará parte de la metodología. Los procesos que incluya la misma, deberá considerar aspectos de gobierno y gestión, procesos de información (entradas, transformación y salidas), el análisis de las estructuras organizativas; principios, políticas y marcos de referencia organizacionales; cultura, ética y comportamiento (como valores compartidos); las personas y sus distintas habilidades; y los servicios, infraestructura y aplicaciones, que en conjunto conforman el sistema de información.



ECU@RISK V.1

UNA METODOLOGÍA PARA LA GESTIÓN DE RIESGO

Capítulo 7: Propuesta metodológica

Introducción

Luego de haber estudiado las metodologías Magerit, Octave-S, CRAMM y Microsoft Risk Management, en los capítulos anteriores, su respectiva alineación con cada una de las ISO, además de haber indagado sobre algunas leyes que amparan la protección de datos contra divulgación, vigilancia o delito; el presente capítulo pretende proponer una metodología de seguridad de la información para la gestión del riesgo informático, aplicable a las MPYMES ecuatorianas, el mismo que se compone en 4 secciones básicas:

1. Parte A: La introducción al manejo de riesgo
2. Parte B: El marco de gestión de riesgo
3. Parte C: El proceso de gestión de riesgo
4. Parte D: Recursos

Parte A: Introducción al manejo del riesgo

La metodología *ECU@Risk* parte de una necesidad clave: Las organizaciones MPYMES ecuatorianas no están preparadas, o aún mantienen niveles de tipo Ad-Hoc en cuanto a gestión de riesgo se refiere.

La academia, específicamente la Universidad, comprende la enseñanza, la investigación y algunas actividades comerciales en relación a un amplio espectro de disciplinas, entornos y escenarios. La diversidad de opiniones y puntos de vista crean un complejo ambiente en el que el riesgo se vuelve inminente; y esto hace que un emprendimiento informático identifique este tipo de situaciones como una oportunidad al cambio, en el que se presenta un desafío, un desafío sobre todo crítico en cuanto a preservar y proteger la información y los recursos que mantiene.

Por otro lado, un estudio a 50 instituciones del preámbulo nacional, con diferentes ejes de negocio, ha revelado que la gestión de riesgo aún es un tópico desconocido, o que, a pesar de ser conocido, no se tiene la cultura de gestionar el riesgo como se debería; o simplemente, el grado de exigencia de las normativas internacionales hace que muchos de estos retos se vuelvan inalcanzables en la práctica.

Todas las actividades empresariales, organizacionales, institucionales, y porque no, personales, involucran riesgo. Es un proceso que debería ser comunicado continuamente y consultado con la parte interesada, además de ser monitoreado y revisado en conjunto con todos los componentes que lo conforman.

Esta metodología está basada en los principios de la administración de riesgos, provista por los estándares ISO 31000:2009, y en las mejores prácticas de seguridad de la información: ISO 27001, ISO 27002 e ISO 27005, además del estudio de las principales metodologías internacionales usadas para la gestión del riesgos y seguridad de la información.

El presente manual provee detalladamente los principios y procesos necesarios para la identificación y valoración de activos y amenazas, el cálculo de riesgo, la identificación de las contramedidas y el establecimiento de políticas de seguridad política.

Estándar de Gestión de Seguridad

Las ISO mencionadas en este documento, 27001, 27002, 27005 y 31000, contribuyen en la definición de lineamientos para el aseguramiento de la información, así como la gestión adecuada de los riesgos que podrían presentarse. De acuerdo con el estándar ISO 31000, *"El logro de la gestión de riesgo dependerá de la efectividad del manejo de la metodología provista por los fundamentos y consideraciones que deberían ser adoptadas en la organización en todos sus niveles",* dentro de la norma, riesgo, gestión, y gestión de los riesgos, son ampliamente utilizados. De manera general:

Principios	**Qué se quiere garantizar**
Crear y proteger el valor	La metodología desarrollada desde el punto de vista universitario puede perseguir objetivos estratégicos demostrables mediante la investigación, el aprendizaje y la enseñanza, su cooperación con la industria, y la participación de la comunidad.
Es una parte integral de los procesos organizacionales	En todo proceso organizacional el riesgo siempre está presente. Es así que la metodología de gestión de riesgo debe considerar adaptarse a la gobernabilidad, las estrategias empresariales y operacionales, la planeación y la gestión, las políticas, los valores y la cultura.
Es parte de la toma de decisiones	Cada individuo de la institución debe conocer que la empresa u organización es liderada generalmente por su Gerente General o por un Director General, ejecutivos que son los responsables de tomar decisiones en base a correctos elementos de juicio, además de priorizar las acciones, y reconocer que cualquier alternativa tomada tiene sus consecuencias.
Es sistemática, estructurada y temporal	El riesgo debe ser tratado de una forma sistemática, estructurada, y saber que eso tiene una fecha de caducidad. Una metodología debe ser consistente, clara y debe permitir alcanzar resultados comparables y confiables.
Está basada en la mejor información disponible	En base al juicio y discernimiento, quienes toman las decisiones deben considerar la información disponible, la experiencia, los pronósticos y la retroalimentación de la parte interesada.
Debe ser adaptada en el contexto interno y externo	Los responsables consideran los mandatos legales y operacionales, los requisitos y expectativas de las entidades reguladoras tanto internas como externas, auditores,

	proveedores de fondos, de gobierno, autoridades y organismos; y dar cuenta de los planes estratégicos institucionales y su perfil de riesgo.
Considera factores humanos y culturales	Una metodología debe considerar las capacidades, percepciones e intenciones del usuario interno y externo, que pueden facilitar o entorpecer el alcance de los objetivos empresariales.
Es transparente e inclusiva	La gestión de riesgo debe ser transparente para la parte interesada, las entidades de control y los tomadores de decisiones.
Es dinámica, iterativa y sensible al cambio	Debe responder constantemente a los cambios. Para ello, debe ser evaluada permanentemente
Facilita la implementación continua de la organización	Es inminente que una metodología para la gestión de riesgo debe trabajar a la par con las estrategias empresariales, a manera de apoyar a la empresa a alcanzar los objetivos que podrían verse impedidos debido a los riesgos y amenazas de entorno que se presentan. Por ello, es mandatorio el comunicar constantemente los eventos relacionados con la gestión de riesgos.

Ilustración 14: Elementos de la gestión de riesgo. Fuente: (University of Adelaide, 2015). Desarrollado por: El Autor

Las organizaciones de toda se encuentran inmersas en desafíos que deben superar, en ámbitos naturales, políticos, socio económicos y culturales, los cuales hacen que los entornos operativos se vuelvan inciertos. Estas influencias podrían impactarlas y hacer que las metas no puedan ser alcanzadas. Este efecto de incertidumbre que se presentan sobre los objetivos organizacionales es conocido como riesgo.

De esta manera, se puede afirmar que:

- La gestión de riesgo se refiere, de manera colectiva, a los principios, metodología y procesos para la administración adecuada de los riesgos, y
- Gestionar riesgos se refiere a la aplicación de estos principios, metodología y procesos para riesgos en particular.

Esta metodología, en base a la fundamentación de (Cavoukian, 2013), considera los siguientes principios de privacidad en espacios públicos, acotando que estos espacios son lugares donde existe afluencia de personal externo a la institución, por ejemplo, el área de atención al cliente o el área de cajas que tiene una institución financiera.

1. La recopilación de los datos por parte de la empresa debe limitarse a lo absolutamente necesario para cumplir con los objetivos que plantea, pero sometida a controles para su retención, uso posterior y divulgación.
2. La empresa debe estar consciente y ser responsable por sus prácticas de gestión y manipulación de información.
3. Cumplir con las reglas de privacidad y restricciones que deberían ser objeto de un escrutinio independiente.
4. Para que la fuerza policial pueda implementar cualquier tipo de vigilancia intrusiva, deberá ser supervisada bajo un sistema bajo autorización judicial previa.
5. Aun donde las emergencias genuinas se vuelvan impracticables para que la policía pueda obtener autorización judicial antes de emplear medidas de vigilancia, el estado debe seguir siendo transparente y responsable por el uso de poderes intrusivos mediante el posterior, oportuno e independiente escrutinio de su uso.
6. Prácticas de vigilancia que se introduzcan en la intimidad mediante el aprovechamiento de nuevas plataformas tecnológicas o procesos de transmisión debe ser analizados detenidamente para garantizar que vayan acompañados de una suficiente rigurosidad de privacidad y protecciones a la rendición de cuentas.
7. Se requerirá la vigilancia eterna para asegurar los derechos fundamentales, incluyendo el derecho a la intimidad personal en relación a todos los espacios públicos, incluidos los que se encontraron en línea y en otros espacios virtuales.

La gestión de riesgo se refiere a las actividades coordinadas que una organización toma para dirigir y controlar el riesgo. La gestión de riesgo puede considerarse como una herramienta para incrementar el valor de un activo de información, o para protegerlo, o simplemente para cualquiera de ambos casos. Las acciones, procesos y controles apoyan a los encargados de la gestión de riesgos a coordinar acciones que permita planificar, identificar, inventariar, gestionar y monitorear los activos de información y los riesgos y amenazas que podrían presentarse, para considerar alternativas de mitigación que permitan asegurar la integridad y confidencialidad de la información y garantizar la disponibilidad de la misma.

Es importante considerar que, cuando la gestión de riesgos es eficaz, esta generalmente pasa desapercibida. Cuando está ausente o falla, el impacto generalmente es muy visible y se la siente sobre toda la organización, y no solo en una agencia, sucursal, facultad, o a nivel de proyecto.

Para una MPYME, la marca y la reputación son muy importantes; el daño a las mismas puede ir, desde transitorias hasta permanentes, pudiendo afectar el número de clientes, la moral del personal y el compromiso con la comunidad.

Una empresa, organización o institución del sector MPYME está influenciada por factores tanto internos como externos. Entre ellos se pueden indicar los siguientes:

- Cambios políticos (entorno externo) y cambios de gobierno corporativo (entorno interno)
- Recortes presupuestales, inestabilidad de la economía global, riesgos monetarios, sostenibilidad financiera y uso de recursos limitados.
- Globalización y la revolución digital.
- Nuevas opciones, tendencias y moda; lo que genera una presión por parte de los clientes y el personal.
- El alto costo de equipamiento para satisfacer las necesidades del mercado y crear ventaja competitiva.

- El escrutinio cada vez mayor y la exigencia de la diligencia, la transparencia y la rendición de cuentas; regulaciones gubernamentales, el seguimiento y la supervisión; auditorías periódicas de organismos externos, y una amplia gama de requisitos reglamentarios, legislativos y obligaciones contractuales que controlen aspectos de las operaciones de la MPYME y la exigencia de las mejores prácticas.

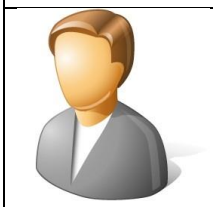
Parte B: El marco de gestión de riesgo

Una metodología para la gestión de riesgo debe integrar, de manera efectiva, todos los procesos que permiten administrar el riesgo en todos los niveles de gobierno institucional, la planeación y estrategias, los procesos de presentación de informes, políticas, valores y la cultura.

Para que el marco de gestión de riesgo sea efectivo, se deberán identificar los roles y responsabilidades del personal que debería soportar y participar en el proceso de gestión de riesgo. Ecu@Risk propone los siguientes roles clave:

	**Alta Dirección**. La alta dirección, en cualquier tipo y tamaño de organización, bajo el estándar de protección y la responsabilidad de cumplimiento de la misión, debe asegurarse de proporcionar los recursos necesarios para desarrollar las capacidades necesarias de manera efectiva, que permitirán llevar a cabo la misión. Además, estarán a cargo de la evaluación continua e incorporación de los resultados de la actividad de evaluación de riesgos en el proceso de toma de decisiones. Un programa de gestión de riesgos eficaz, que evalúa y cubre los riesgos relativos a la misión de TI, requiere el apoyo y la participación de este actor clave.

	**Propietarios de información:** Son los responsables gestionar la información, así como aprobar el acceso a la misma, validando que los controles adecuados para este fin se encuentran vigentes, con el fin de garantizar la confidencialidad e integridad de la información. Generalmente, el propietario de información es el gerente, subgerente o jefe de área. Así que, como actividad adicional, deberán aprobar y firmar en cambios en sus sistemas de TI (por ejemplo, el sistema de mejora, los principales cambios en el software y hardware). Por lo tanto, los propietarios de la información deben entender su papel en la gestión de riesgos procesar y apoyar plenamente este proceso.
	**Propietario(s) de sistemas de información:** El o los propietarios del sistema de información son los responsables implementar y de asegurar que los controles adecuados están implementados y funcionando, para garantizar la integridad, confidencialidad y disponibilidad de los sistemas de información y de datos que poseen. Son responsables de los cambios en sus sistemas. En una MPYME generalmente es el técnico encargado de sistemas, o el jefe departamental de TI.
	**Comité de Riesgo de Tecnología de Información (CRTI).** La responsabilidad de comité es el de evaluar la planificación de riesgo tecnológico y de información, y monitorear la gestión del rendimiento, incluyendo los componentes de seguridad de la información. Las decisiones que se tomen en esta área deben estar basados en un adecuado programa de gestión de riesgo.
	**Coordinador de Seguridad designado (CSD)**: El coordinador de programas de seguridad de información es el responsable designado por el comité de Riesgo de Tecnología de Información para los programas de seguridad de sus organizaciones, incluyendo la gestión de riesgos. Por lo tanto, juega un papel destacado en la introducción de una metodología adecuada, estructurada para apoyar en la identificación, evaluación y minimización los riesgos a los sistemas

	informáticos que apoyan la misión organizacional. El CSD también actúan como consultores principales en apoyo de la alta gestión para asegurarse de que esta actividad se lleva a cabo de manera continua. No puede ser parte del departamento o el área de TI por razones éticas y por funciones incompatibles.
	**Profesionales de TI - Proveedores de soluciones tecnológicas (PST):** Conformado por profesionales de TI (por ejemplo, ingenieros en redes de datos, proveedores del sistema informático, proveedores de aplicaciones, bases de datos y administradores; especialistas en informática; analistas de seguridad; consultores de TI), son responsables de la correcta aplicación de los requisitos en sus sistemas de TI.
	**Auditor de TI:** Velar por el cumplimiento de las políticas, la normativa, y el control de los servicios de TI; determinando si estos son adecuados y si permiten alcanzar los objetivos y estrategias planteados.
 	**Comité de certificación de TI:** A medida que se producen cambios en el sistema de información existente, por ejemplo, la expansión de la conectividad de red, el cambio de infraestructura de servidores de información existentes, la modificación de la estructura institucional, o la introducción de las nuevas tecnologías, los profesionales de TI (Proveedores de soluciones tecnológicas) más los miembros del comité de Riesgo de TI, deben validar los cambios realizados, a manera de identificar y evaluar nuevos riesgos potenciales, para así sugerir la implementación de nuevos controles de seguridad según sea necesario, para salvaguardar las plataformas y sistemas de tecnologías de información.

Parte C: El proceso de gestión de riesgo

La gestión del riesgo ya no es un elemento opcional: es una consideración necesaria cada vez que se toma una decisión, ya sea para desarrollar una relación, iniciar un proyecto o realizar un evento, con lo que permitirá alcanzar una buena calidad de los resultados. Debe alinearse constructivamente a las actividades diarias y la toma de decisiones con los objetivos y resultados que ayudarán a alcanzar los objetivos estratégicos, o ejecutar con éxito los planes operativos propuestos. Al gestionar el riesgo, se aplica la norma de la manera descrita aquí.

Así, debe considerarse el entorno en el que se desenvuelve la MPYME, a manera de seleccionar las contramedidas más adecuadas.

La gestión de riesgo, está conformada por cuatro grandes etapas:

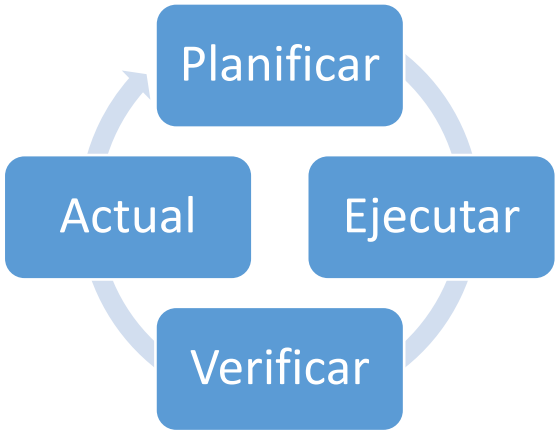


Ilustración 15: El proceso de gestión de riesgo basado en el modelo de Deming. Elaborado por: El autor

Esta metodología se resume en 5 procesos de gestión, 1 proceso de monitoreo y control, y 1 proceso comunicacional. La siguiente sección presenta el proceso de gestión de riesgo estándar que deberá seguir una organización, empresa o institución en su aseguramiento de la información.

Paso 1: Determinación del contexto

Es importante verificar el entorno en el que se desenvuelve la empresa. Este primer paso consiste en identificar el tipo de organización, y su tamaño. Consecuentemente, habrá que definir el alcance de la investigación y sus objetivos; es decir, qué actividad, decisión, proyecto, programa, o cuestión requiere un análisis. Es importante además identificar a los interesados y/o áreas pertinentes involucradas o afectadas, así como los factores internos y el ambiente externo. Los siguientes procesos (PEC) hacen referencia a: Procesos para establecer el contexto.

PEC-01: Procedimiento para la identificación del tipo y tamaño de organización

1. Determinar la clasificación de su organización de acuerdo a la tabla provista a continuación:

Según el Servicio de Rentas Internas, en Ecuador las sociedades se dividen en privadas y públicas, y éstas a su vez se dividen en:

Clasificación	Consideraciones
a. Privadas: Son personas jurídicas de derecho privado	Aquellas que se encuentran bajo el control de la Intendencia de Compañías como por ejemplo las Compañías Anónimas, de Responsabilidad Limitada, de Economía Mixta, Administradoras de Fondos y Fideicomisos, entre otras. Aquellas que se encuentran bajo el control de la Superintendencia de Bancos como por ejemplo los Bancos Privados Nacionales, Bancos Extranjeros, Bancos del Estado, Cooperativas de Ahorro y Crédito, Mutualistas, entre otras. Otras sociedades con fines de lucro o Patrimonios independientes, como por ejemplo las Sociedades de Hecho, Contratos de Cuentas de Participación, entre otras.

	Sociedades y Organizaciones no gubernamentales sin fines de lucro, como por ejemplo las dedicadas a la educación, entidades deportivas, entidades de culto religioso, entidades culturales, organizaciones de beneficencia, entre otras. Misiones y Organismos Internacionales, como embajadas, representaciones de organismos internacionales, agencias gubernamentales de cooperación internacional, organizaciones no gubernamentales internacionales y oficinas consulares.
b. Públicas: Son personas jurídicas de derecho público	Del Gobierno Nacional, es decir las funciones: Ejecutiva, Legislativa y Judicial. Organismos Electorales Organismos de Control y Regulación Organismos de Régimen Seccional Autónomo, es decir Consejos Provinciales y Municipalidades Organismos y Entidades creados por la Constitución o Ley Personas Jurídicas creadas por el Acto Legislativo Seccional (Ordenanzas) para la Prestación de Servicios Públicos. El Catastro de instituciones, entidades, empresas y organismos descentralizados del Estado es gestionado y administrado por el Ministerio de Relaciones Laborales. Para información con mayor detalle, por favor referirse a la página oficial del Ministerio de Trabajo a la siguiente dirección URL: http://www.trabajo.gob.ec/catastro-instituciones-del-sector-publico/

c. Contribuyentes Especiales	Los contribuyentes especiales son asignados por la Administración Tributaria en función de su importancia económica, conforme al análisis realizado por parte de la Dirección Nacional de Gestión Tributaria. Todos los contribuyentes que tengan esta característica tendrán obligaciones tributarias distintas a las demás sociedades.

Tabla 8: Clasificación de las sociedades. Fuente: SRI. Elaborado por: El autor

PEC-02: Procedimiento para identificar el tamaño de la empresa

Matriz para la identificación del tamaño de empresa

Tipo	Consideraciones
Microempresa	El número de empleados es igual o menor a 10 personas. El volumen anual de negocio no supera los 20 mil dólares.
Pequeña empresa	El número de empleados es mayor a 50 personas. El volumen anual de negocio supera los 20 mil dólares.
Mediana empresa	Alberga entre 50 a 99 empleados Su capital fijo no debe sobrepasar los 120 mil dólares.

Tabla 9: Clasificación de la organización por su tamaño. Fuente: (Vásquez & López, 2016) (Muñoz, 2012). Elaborado por: El autor

PAO-01.1. Utilizar la herramienta de análisis PESTEL:

Los procesos PAO (Procesos de Análisis Organizacional), hacen referencia a que, para implementar un proceso de gestión de riesgo dentro una organización del sector MPYME, será necesario partir de un ***análisis PESTEL***. Este análisis considera factores ***P***olíticos, ***E***conómicos, ***S***ocio-culturales, ***T***ecnológicos, ***E***cológicos o ambientales, y ***L***egales; los mismos que afectan de una u otra manera a la organización y consecuentemente a su desarrollo.

Antes que nada, considere realizar la siguiente pregunta: *¿Lo que se está evaluando se trata de una nueva asociación, programa, proyecto o tal vez un evento?* De esta manera se busca establecer el alcance o ámbito de la evaluación del riesgo.

Para realizar el análisis PESTEL, considerando a (Azanza & Bermeo, 2016), se recomiendan los siguientes pasos:

Paso 1.

Definir y elegir el método apropiado para su organización. Se puede utilizar una de las siguientes opciones:

- Realizar un análisis descriptivo mediante investigaciones de mercado.
- Elaborar un taller, en el cual se debe reunir a los involucrados del comité de Riesgo de Tecnologías de información, y entre todos realizar el análisis con una lluvia de ideas. Es necesario para este método, definir un moderador y un grupo focal.

Una vez elegido el método adecuado para su organización, continúe con el paso 2.

Paso 2.

Delimitar la cobertura de la empresa en el país, siendo este:

- Local
- Regional
- Nacional

- Internacional

Una vez que se ha identificado el alcance de la organización, se procederá con el siguiente paso.

Paso 3.

De acuerdo a los siguientes lineamientos, investigar los componentes de cada uno de los factores del análisis PESTEL:

- Factor ***P***olítico.- se recomienda considerar los estudios de riesgo político que cada año son realizados por "AON" y por "MARSH", empresas internacionales dedicas al análisis mundial de riesgos (Azanza & Bermeo, 2016), sin descuidar el observatorio PYME de la Universidad Andina Simón Bolívar.

- Factor ***E***conómico.- Es clave evaluar los "Indicadores Económicos del Banco Central del Ecuador", donde, entre otros aspectos, se podrá encontrar información relacionada con tasas de interés, el producto interno bruto - PIB, el nivel de inflación, etc. (Azanza & Bermeo, 2016) también sugieren examinar los datos económicos que publica el Instituto Nacional de Estadísticas y Censos (INEC) relacionados al sector de interés, con el fin de conocer el estado económico del país y determinar su influencia en la organización.

- Factor ***S***ocio–cultural.- El INEC presenta información sobre el "Censo de población y vivienda", lo que permite conocer los cambios del nivel poblacional, y con ello habilita el predecir comportamientos de consumo local, nacional e internacional, en base a la "Encuesta de Estratificación del Nivel Socioeconómico" (Azanza & Bermeo, 2016), por lo tanto será importante y fundamental considerarlo dentro del análisis de riesgos.

- Factor ***T***ecnológico.- Considerar los cambios tecnológicos y su evolución es trascendental, ya que estos de una forma u otra afectan a la industria donde compite la organización. Para ello, (Azanza & Bermeo, 2016) proponen

analizarlo en base a la información ofrecida por el INEC en su documento de estudio "Principales indicadores de Actividades de Ciencia, Tecnología e Innovación".

- Factor ***E***cológico.- Las regulaciones ambientales son aspectos relevantes, que inciden inclusive en la imagen de la empresa. Para ello será importante identificar las leyes de protección del medio ambiente, las regulaciones enfocadas al consumo de energía y agua, a elementos no renovables, al reciclaje de residuos, y la mitigación del impacto ambiental. Se sugiere establecer el contexto empresarial en base a la información proporcionada por el Ministerio del Ambiente del Ecuador. (Azanza & Bermeo, 2016)

- Ámbito ***L***egal.- son aquellas normativas que afectan al restaurante, en el que se hallan inmersos el "Código del trabajo", las licencias y permisos requeridos por el área local, además del "Reglamento de seguridad y salud de los trabajadores y mejoramiento del medio ambiente de trabajo" y la "Ley Orgánica de Salud". (Azanza & Bermeo, 2016).

Una vez definidos los factores se prosigue a llenar el *Cuadro de análisis PESTEL*, para lo cual se deberán considerar los pasos definidos a continuación:

Paso 4.

Analizar los componentes de los factores ***PESTEL***, diferenciándolos de acuerdo a cada una de las perspectivas que la conforman, lo que permitirá identificar los que inciden directamente a la organización. Para ello, (Azanza & Bermeo, 2016) sugieren plantear los siguientes cuestionamientos:

¿Qué factor es el que afecta como empresa/organización/institución?

¿Qué factor denota relevancia para la empresa/organización/institución?

Paso 5.

Es importante evaluar los factores externos de la organización, mediante el análisis las amenazas u oportunidades, para lo cual se puede plantear la siguiente pregunta:

¿El factor estudiado generaría una oportunidad o una amenaza para la empresa?.

De esta manera, las amenazas podrán ser tratadas como riesgos, y las oportunidades como posibles contramedidas.

Paso 6.

Priorizar las amenazas y las oportunidades de los todos los factores (siendo 1 el más importante), es decir, establecer la prioridad para cada una de las amenazas identificadas de manera general, independientemente del factor al cual pertenezca. Repita el procedimiento considerando las oportunidades. La prioridad se debe fundamentar en el grado de afección que considera que tiene el factor hacia la organización. (Azanza & Bermeo, 2016)

CUADRO DE ANÁLISIS PESTEL PARA _(Nombre de la organización)_				
FACTOR	**DESCRIPCIÓN**	**CONDICIÓN**		**P**
POLÍTICO		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
ECONÓMICO		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
SOCIO-CULTURAL		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
TECNOLÓGICO		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
ECOLÓGICO		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
LEGAL		O	A	
		O	A	
		O	A	
		O	A	
		O	A	
OBSERVACIONES				
SIMBOLOGÍA: P = PRIORIDAD; O = OPORTUNIDAD; A = AMENAZA				

Tabla 10: Cuadro de análisis PESTEL. Fuente: (Azanza & Bermeo, 2016)

Establecer el contexto interno

Será necesario identificar el contexto interno de la empresa, especialmente en la identificación de roles y responsabilidades de los empleados, componentes salariales, compromiso para con la empresa, nivel de madurez profesional. También será importante delimitar las áreas de trabajo sensible, mecanismos de comunicación internos, conocimiento sobre el nivel de políticas institucionales, entre otros factores. La siguiente sección explica los procedimientos necesarios para conseguir este objetivo.

PAO-01.2. Utilizar la herramienta de análisis FODA para la matriz EFI:

Para realizar el análisis interno, será necesario primeramente recabar las Fortalezas y Debilidades institucionales, considerando la matriz planteada a continuación, la misma que posteriormente será completada con las Oportunidades y Amenazas identificadas en el proceso MPS-01.1.

FODA PARA (NOMBRE DE LA ORGANIZACIÓN)

Fecha:		
Elaborado por:		
Aprobado por:		
Aspectos positivos	**Aspectos Negativos**	
FORTALEZAS - - -	**DEBILIDADES** - - -	**De origen Interno**
OPORTUNIDADES - - -	**AMENAZAS** - - -	**De origen Externo**

Tabla 11: Matriz para identificación del FODA institucional. Fuente: (Azanza & Bermeo, 2016)

PAO-01.2. Utilizar la herramienta de análisis McKinsey para el análisis Interno

El objetivo de este procedimiento es identificar los perfiles, actividades y roles de los colaboradores de la empresa; así como el de identificar su nivel de conocimiento sobre políticas y procedimientos organizacionales. McKinsey proporciona una herramienta basada en las 7S institucionales: Staff (personal), Structure (Estructura), Skills (Habilidades), System (políticas y procedimientos internos), Shared Values (Valores compartidos, como misión, visión, ética, valores), Strategy (Estrategias) y Style (Estilo de dirección). En la teoría de las 7S de McKinsey se argumenta que, si una de las S falla, el resto falla; y por lo tanto no se logra la continuidad del negocio. Esto dará una idea más clara en el siguiente proceso, que consiste en la identificación de riesgos.

Para el análisis puntual del objetivo planteado, se seleccionará el personal, habilidades, sistema y valores compartidos. Con estos argumentos, será importante considerar las siguientes actividades.

Paso 1: Solicite el listado de personal al encargado de gestión de recursos humanos, así como también identifique el tipo de estructura orgánico funcional y la ubicación del recurso en ese organigrama en base a su experiencia y perfil.

Paso 2: Evalúe puestos con roles incompatibles. Por ejemplo, un cajero de banco podría realizar transacciones de depósito y/o retiro, pero nunca creación y/o eliminación de cuentas. Ingrese la información recopilada en la “Matriz para identificación de roles y actividades incompatibles “, la misma que se expone a continuación.

Matriz para identificación de roles y actividades incompatibles			
Fecha:			
Departamento:			
Nombre del Funcionario evaluado:			
Jefe inmediato:			
Cargo:			
Proceso	Funciones	Roles incompatibles	Observaciones
Elaborado por:			
Revisado por:			
Aprobado por:			

Tabla 12: Matriz para identificación de roles y actividades incompatibles. Fuente: Autoría Propia

Paso 3: Una vez identificados los roles y actividades incompatibles, será importante realizar un análisis de los cargos de cada uno de los miembros del equipo de trabajo. Para ello, considere utilizar la matriz a continuación

Matriz para identificación de habilidades			
Fecha:			
Departamento:			
Nombre del Funcionario evaluado:			
Jefe inmediato:			
Cargo:			
Perfil		Actividades directas	
		*	
		*	
		*	
		Actividades indirectas	
		*	
		*	
		*	
		Actividades incompatibles	
		*	
		*	
		*	
Elaborado por:			
Revisado por:			
Aprobado por:			

Tabla 13: Matriz para la identificación de habilidades. Fuente: Autoría propia

Es importante considerar identificar el perfil de cada uno de los empleados (en la columna "Perfil"), incluyendo su título profesional, título de magister (en caso de que aplique),

trayectoria profesional. En la columna siguiente, relacione las actividades identificadas en la "Matriz para identificación de roles y actividades incompatibles", ubicándolas en las secciones respectivas: "Actividades directas" (lo que habilita su campo profesional más la experiencia), "Actividades indirectas" (lo que podría hacer como consecuencia de su trayectoria experimental), "Actividades incompatibles" (que no tienen relación con su campo profesional o experiencia).

Paso 4: Recabe información sobre la misión, visión, valores y objetivos corporativos

Valores compartidos organizacionales	
Misión	*
Visión	*
Valores	* * *
Objetivos institucionales	* * *

Tabla 14: Matriz para la identificación de Valores compartidos organizacionales. Fuente: Autoría propia

Paso 5: **(A ser llenado en conjunto con la Alta gerencia, la dirección o el propietario del negocio)** Es fundamental indagar sobre el estilo empresarial y el estilo que genera la alta dirección sobre la empresa, por cuanto tiene una influencia directa sobre el personal, proveedores y clientes en general. Haciendo referencia a una de las 7S de McKinsey, responda las siguientes preguntas, donde 1 es "Muy Bajo" y 5 es "Muy Alto".

Matriz de identificación del estilo organizacional

Cuestionamientos	1	2	3	4	5
¿La rotación del personal en la empresa es?					
¿La empresa tiene empleados con exceso de trabajo?					
¿Existen situaciones de controversia entre los empleados?					
¿El índice de reclamos por parte de los clientes es?					
¿El número de empleados que trabaja horas adicionales es?					

Tabla 15: Matriz de identificación del estilo organizacional. Fuente: Autoría Propia

En la siguiente sección de la matriz considere los siguientes niveles:

1: "nunca"

2: "Casi nunca"

3: "A veces"

4: "Con frecuencia"

5: "Siempre"

Matriz de identificación del estilo organizacional					
Cuestionamientos	1	2	3	4	5
¿La gerencia general tiene reclamos por parte de sus empleados?					
¿Los clientes han reclamado por mala atención del personal?					
¿Los clientes han reclamado por productos defectuosos?					
¿Los clientes han reclamado por negligencia?					
¿Se han producido robos internos?					
¿La empresa ha sido víctima de actos fraudulentos?					
¿La empresa ha sido víctima de sabotajes de información?					
Los valores compartidos organizacionales son transmitidos (durante el año):					
Ha realizado evaluaciones a sus empleados a fin de determinar el nivel de conocimiento sobre los valores compartidos					

Tabla 16: Matriz de identificación del estilo organizacional. Fuente: Autoría propia

Los indicadores anteriormente evaluados, dan una referencia sobre el entorno en el que se desenvuelve la organización. Una vez alcanzada etapa, se puede iniciar con la siguiente etapa de la metodología.

Paso 2: Identificar los activos de información

Los activos de información, en una organización, hace referencia a cualquier elemento que contenga información. ECU@risk plantea los siguientes grupos de clasificación de activos de información que deberán ser considerados:

(ED)	Edificaciones
(HW)	Hardware
(SW)	Software
(IE)	Información electrónica
(IP)	Información en papel
(Extraible)	Medios de almacenamiento extraible
(IC)	Infraestructura de comunicaciones
(RRHH)	Recursos humanos

Ilustración 16: Clasificación de los activos de información

El procedimiento para la identificación de los activos de información se detalla a continuación:

IA-01.1. Identificar activos de información

El proceso IA, (Identificación de activos) brinda las secuencias y recomendaciones para identificar los activos de información, los mismos que se han establecido en la figura 13: "***Clasificación de los activos de información***".

Paso 1: Para iniciar con la identificación de los activos de información, revise primeramente la tabla de clasificación para cada uno de las categorías indicadas anteriormente, la misma que se describe en esta sección:

Edificaciones

(ED)	Edificaciones		
Clasificación		Sub clasificación	Observaciones
(CPD)	Centro de cómputo principal		En una empresa del sector MPYME, generalmente las micro y pequeñas cuentan con uno o dos servidores de aplicaciones, que se encuentran ubicados por lo general en el área administrativa. En una mediana empresa, el centro de cómputo por lo general es un cuarto independiente.
(CPA)	Centro de procesamiento alterno		
(AT_CLI)	Espacio público de atención al cliente		
(CONTA)	Área de contabilidad		
(SEN)	Área restringida (o áreas sensibles, hace referencia a lugares físicos de la edificación que son de acceso	Hospitales: • (QUI) Quirófano • (UCI) Unidad de cuidados intensivos • (RAYX) Unidad de rayos X	

	restringido o limitado, o que puede estar sujeta a restricciones)	• (TOMOGRAFIA) Unidad de tomografía • (FARM) Farmacia • (CAJA) Área de cajas • (EME) Área de emergencias • (PED) Área de pediatría • (NEO) Área de Neonatología • (OTRO) Otras áreas sensibles Entidades financieras: • (ET) Emisión de tarjetas • (BOVEDA) Bóveda de valores • (CAJA) Área de cajas • (CTE) Área de procesamiento de cámara (cheques) • (OTRO) Otras áreas sensibles Entidades comerciales: • (BDG) Bodega • (CAJA) Área de cajas • (OTRO) Otras áreas sensibles Entidades industriales: • (PLANTA) Planta de producción • (BDG) Bodega • (TALLER) Espacio	

		para taller de construcción y/o reparación • (OTRO) Entidades educativas: • (DIR) Dirección • (COCINA) Área de cocina • (AULA) Aulas • (PF) Área de atención a padres de familia	
(GER)	Gerencia		
(FIN)	Área financiera		
(VENTAS)	Área de ventas		
(SEG)	Área de seguridad y vigilancia		
(OTRO)	Otras áreas no contempladas		Describir las áreas no contempladas utilizando una codificación adicional para cada espacio no considerado en este documento. Ejemplo: (OTRO)(MKT), lo que haría referencia al área de Marketing.

Por ejemplo, en caso de hacer referencia al Quirófano 1 de un hospital, se debería clasificar y codificar el activo de información de la siguiente manera:

(ED)(SENS)(QUI)(01)

Si existiese un área sensible de un tipo de industria que no esté contemplada en este documento, por ejemplo, la industria de restauración (restaurantes, bares, tenedores), se recomienda realizar el siguiente procedimiento:

1) Identificar el área y rotularla con codificación propia de su organización:
    a. (CLI): Área de clientes
    b. (COCINA): Área de cocina
    c. (CAJA): Área de cajas y cobros

2) Establezca la codificación del ejemplo anterior:
    a. (ED)(SENS)(COCINA)(01)

3) Con ello, haría referencia a: La edificación del restaurante tiene un área sensible que es Cocina. El 01 es un número incremental, único para cada activo de información.

IMPORTANTE!: La codificación del activo de información debe contener:
(COD. CLASIFICACIÓN DEL ACTIVO) (SUB CODIGO) (SUB CÓDIGO) (SECUENCIAL)
El campo secuencial es un número incremental, que permite distinguir a un activo de información frente a otro.

Hardware

Hardware hace referencia a la parte física de un computador. No interesa como activo de información el teclado, pantalla o ratón del computador. A continuación, se expone la clasificación sugerida.

(HW) Hardware			
Clasificación		Sub clasificación	Observaciones
(SVR)	Servidores		Se considera un equipo servidor a un equipo de coste económico medio, tanto en su adquisición como en su mantenimiento.
(PC)	Equipos de escritorio		Se considera como PC a los computadores de bajo costo económico y que son de fácil remplazo
(LAPTOP)	Computadores móviles (laptops)		
(CELULAR)	Teléfonos celulares no inteligentes		
(SMART)	Teléfonos celulares inteligentes		Se considera un teléfono celular como inteligente si tiene la capacidad de navegar por internet, gestionar aplicaciones, contar con herramientas para gestionar documentos. Usualmente cuentan con un sistema operativo Android, iOS o Windows.
(PRINT)	Impresoras		
(SCAN)	Escáneres		
(MULTI)	Impresoras multifuncionales		Una impresora multifunción es aquella que tiene capacidad de escanear e imprimir.
(FAX)	Sistemas de transmisión FAX		
(FW)	Firewall		

Software

Hace referencia a las aplicaciones, programas o sistemas informáticos, en los cuales se incluye el sistema operativo, las hojas de cálculo, un procesador de texto, el sistema contable, el navegador de internet, etc.

(SW) Software			
Clasificación		Sub clasificación	Observaciones
(PROPIO)	Desarrollo propio		Software elaborado dentro de la empresa. Lo que busca asegurar es su código fuente y propiedad intelectual
(SUB)	Desarrollo sub contratado		Software elaborado a medida para la empresa, por terceros.
(STD)	Software estándar.		Software comercial adquirido (vea la subclasificación siguiente)
	(OFI)	Paquetes ofimáticos	Excel, Word, Libre Office, entre otros, pueden ser considerados como paquetes ofimáticos
	(CLIEMAIL)	Cliente de correo electrónico	Como cliente de correo electrónico puede ser considerado Outlook, Entourage.
	(SRVMAIL)	Servidor de correo electrónico	Usualmente en una MPYME el servicio de correo es provisto por terceros (Ej. Gmail)
	(OS)	Sistema operativo	Sistema Operativo: (Ej. Windows, Linux)
	(AV)	Antivirus	
	(BACKUP)	Respaldos	Sistema de respaldos
	(DBMS)	Gestor de base de datos	El gestor de base de datos puede ser: Oracle, MySQL, SQL Server, Access.

Información electrónica

La información electrónica está conformada por los archivos, ya sean resultados del manejo de una hoja de cálculo, de un documento de texto, de un gráfico o fotografía; o también puede ser considerado como un registro de una base de datos. La tabla a continuación describe los elementos a ser considerados.

(IE) Información Electrónica			
Clasificación		Sub clasificación	Observaciones
(ARCHIVO)	Archivos		Se consideran archivos a cualquier documento electrónico.
(COPIA)	Archivos de respaldo		Archivos electrónicos de respaldo (copia del original)
(CONF)	Archivos de configuración		
(CLAVE)	Archivos de contraseñas		
(LOG)	Archivos que contienen el registro de actividades		
(DATA)	Tablas y bases de datos		
(EXE)	Código ejecutable		El código ejecutable generalmente tiene una extensión EXE, o COM, o BAT. Es el resultado de la compilación del código fuente.
(FUENTE)	Código fuente		El código fuente de una aplicación, módulo, componente o sistema.

Información en papel

En una organización, así como existe información electrónica, también existirá información que no lo sea. Es importante considerar los registros en papel, cheques, pagarés, balances, estados financieros, historiales clínicos, resultados de pruebas en talleres; cualquiera de ellos que no sea registrado en un computador o similar, será considerada como información en papel.

(IP) Información en papel			
Clasificación		Sub clasificación	Observaciones
(DOCS)	Documentos		Se consideran documentos a cualquier información escrita en papel
(CARBON)	Copia carbón del documento		Copia en carbón del documento

Medios de almacenamiento extraíble

En una MPYME, se tiene la costumbre de respaldar la información en medios extraíbles. De esta manera, esta categoría hace referencia a CDs, DVDs y últimamente en unidades USB (flash memory, pendrives, discos duros externos).

(EXTRAIBLE) Medios de almacenamiento extraíble			
Clasificación		Sub clasificación	Observaciones
(OPTICO)	Medios de almacenamiento óptico		Son medios de almacenamiento que requieren cuidado en su almacenamiento, además de un lector óptico que permita revisar su contenido
	(CD)	CD Rom	Medios de

			almacenamiento de 640 MB hasta 700 MB
	(DVD)	DVD Rom	Medios de almacenamiento de 4GB hasta 8GB
	(BLUE)	BLUE Ray	Medios de almacenamiento de 10GB
(ELECTRONICO)	Medios de almacenamiento electrónico		Medios de almacenamiento electrónicos, cuya interfaz es el USB:
	(PEN)	Pen Drive / Flash Memory	
(MECANICO)	(DISCO)		Medios mecánicos extraíbles: Discos duros externos.

IC – Infraestructura de comunicaciones

La infraestructura de comunicaciones está conformada por aquellos elementos que permiten la intercomunicación entre los dispositivos informáticos y electrónicos de la red, así como de los dispositivos que permiten la intercomunicación de voz. La clasificación sugerida de los mismos se expone a continuación.

(IC) Infraestructura de comunicaciones			
Clasificación		Sub clasificación	Observaciones
(ROUTER)	Router		Dispositivo utilizado para la interconexión de computadores y la salida a una red diferente (Ej. Internet)
(SWITCH)	Switch		Dispositivo utilizado para la interconexión de

			computadores.
(HUB)	Hub		Dispositivo utilizado para la interconexión de computadores.
(PBX)	Central Telefónica		
(VOIP)	Voz sobre IP		Dispositivos de voz sobre IP
(MODEM)	Módem		Usualmente es un dispositivo que permite el acceso a Internet.
(WIFI)	Red WiFi		Red inalámbrica
(LAN)	Red LAN		Red de área local (red cableada)

RRHH – Recursos humanos

Hace referencia al personal que forman parte de las actividades diarias de la empresa. La clasificación sugerida es la siguiente:

(RRHH) Recursos humanos			
Clasificación		Sub clasificación	Observaciones
(UE)	Usuario externo		Usuarios externos. Por ejemplo, proveedores o clientes.
(UI)	Usuario interno		Personal de la institución
(TI)	Personal de TI		Personal de tecnologías de información

Paso 2: Para continuar con la clasificación de la información, es necesario que cada activo que haya identificado se registre de acuerdo a cada una de sus categorías, y se las valore de acuerdo a las dimensiones de valoración.

Las dimensiones de valoración son las características o atributos que hacen valioso un activo (Ministerio de Hacienda y Administraciones Públicas de España, 2012). Una dimensión es un aspecto de un activo, independiente de otros aspectos. Se puede realizar el análisis de riesgos centrados en un único aspecto, independientemente de lo que ocurra con otros.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

[D] Disponibilidad

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

¿Qué pasaría si la información de esos activos no estaría disponible cuando se la necesite?

[I] Integridad de los datos

[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

¿Qué pasaría si los datos fueran modificados sin conocimiento y control?

[C] Confidencialidad de la información

[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

¿Qué pasaría si esa información es conocida por personas o sistemas no autorizados?

Paso 3: Una vez determinadas las dimensiones de valoración, es hora de valorarlas de acuerdo a un criterio de valoración.

Según (Ministerio de Hacienda y Administraciones Públicas de España, 2012), para valorar los activos sirve, en teoría, cualquier escala de valores. Para efectos prácticos se debe considerar:

- Usar una escala común para todas las dimensiones, permitiendo comparar riesgos,
- Usar una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas y
- Utilizar un criterio homogéneo que permita comparar análisis realizados por separado

Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

valor	criterio	
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Ilustración 17: Criterios de valoración. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Paso 4: Cada registro deberá considerar, al menos:

Código del Activo	Descripción	(D)	(I)	(C)	Valoración total	Valor

Donde el campo “Valoración total” registrará el valor más alto de la fila. Por ejemplo:

Código del Activo	Descripción	(D)	(I)	(C)	Valoración total	Valor
(HW)(PC)(01)	Equipo de atención al cliente	5	9	4	**9**	

Paso 5: Utilizar la escala de criterios de valoración, complete la última columna.

Código del Activo	Descripción	(D)	(I)	(C)	Valoración total	Valor
(HW)(PC)(01)	Equipo de atención al cliente	5	9	4	**9**	**Muy Alto**

Paso 3: Identificación de los riesgos

Para identificar el riesgo, considere realizar las siguientes preguntas iniciales:

- **Qué puede pasar:** ¿Qué podría ir mal, evitar el logro de los objetivos pertinentes? ¿Qué acontecimientos o sucesos podría poner en peligro los resultados esperados?

- **Cómo puede pasar:** ¿Qué pasó? ¿Es probable que pueda volver a ocurrir? ¿Qué factores podrían accionar su reincidencia?

- **Dónde puede suceder**: ¿Dónde podría suceder? ¿Es probable que el riesgo ocurra en cualquier lugar o en cualquier contexto? ¿O es un riesgo que depende de la ubicación, área física o actividad?

- **¿Por qué podría suceder:** ¿qué factores deben estar presentes para que el riesgo se materialice o vuelva a ocurrir? El comprender por qué un riesgo puede ocurrir o repetirse, es importante si se gestionará el mismo.

- **¿Cuál podría ser el impacto?:** Si el riesgo se materializa, ¿qué impacto o consecuencias se presentan o podrían presentarse? ¿Será que el impacto se sienta solo en un departamento, o se sentiría en toda la organización? ¿Implica aquello consecuencias de reputación o solo financieras?

- **¿Cuál podría ser el impacto?:** Si el riesgo se presentara, ¿qué impacto o que consecuencias podrían resultar? ¿Será que el impacto se sentirá a nivel departamental o tendrá un impacto en toda la organización? Es importante considerar como áreas de impacto: Consecuencias financieras; impacto humano; la prestación de servicios; compromiso con el cumplimiento legal o contrato; y el impacto adverso sobre la marca y la reputación por no cumplir o lograr los objetivos estratégicos.

Siempre que sea posible, proporcione datos cuantitativos y / o cualitativos. Esto ayudará a describir el riesgo o apoyará a la calificación de riesgo. Las fuentes de información pueden incluir los registros anteriores, la experiencia del personal, prácticas de la industria, la literatura y la opinión de expertos.

Amenazas

Su organización deberá continuamente identificar las amenazas que pueden afectar la continuidad de su negocio. Para ello, se utilizará la siguiente guía que propone un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción resumida de lo que puede pasar	
Tipos de activos: Que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** Enumere las dimensiones de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante

Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.

En Ecuador, las amenazas organizacionales pueden estar clasificadas de la siguiente manera:

Ilustración 18: Clasificación de los riesgos de información organizacionales. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012). Desarrollo: Autoría propia.

Los desastres causados por riesgos naturales, pueden considerarse como resumen en la siguiente tabla:

[NATURALES] Errores y fallos no intencionados

[N.*] Desastres naturales	
Activos afectados: • [HW] equipos informáticos (hardware) • [EXTRAIBLE] soportes de información • [ED] edificaciones • [RRHH] recursos humanos	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, aludes, ciclones, avalancha, corrimiento de tierras, incendios e inundaciones	

Los desastres causados a propósito son realizados por los humanos, ya sea de forma deliberada, y pueden ser considerados de acuerdo a la tabla a continuación:

[PROVOCADO] Errores y fallos no intencionados

[PROVOCADO.*] Desastres provocados	
Tipos de activos: • [HW] equipos informáticos (hardware) • [EXTRAIBLE] soportes de información • [RRHH] Recursos Humanos • [ED] edificaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, corte energético accidentes de tránsito, construcción, vibraciones, polvo, suciedad, temperatura, humedad, incendio e inundación. **Origen:** Entorno (accidental) Humano (accidental o deliberado).	

Ilustración 19: Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[NO_INTENCIONADO] Errores y fallos no intencionados

Considerando las especificaciones de (Ministerio de Hacienda y Administraciones Públicas de España, 2012), los fallos no intencionales causados por las personas pueden desencadenar ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto. Origen: Humano (accidental).

[NO_INTENCIONADO.1] Errores de los usuarios	
Tipos de activos: • [IE] Información electrónica • [IP] Información en papel • [SW] aplicaciones (software) • [EXTRAIBLE] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: Errores involuntarios de personas cuando usan los servicios, datos, etc.	

Ilustración 20: Errores de los usuarios. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[NO_INTENCIONADO.2] Errores del administrador	
Tipos de activos: • [IE] información electrónica • (IP) Información en papel • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [IC] Infraestructura de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad

Descripción: Errores involuntarios de personas con responsabilidades de instalación y operación.

Ilustración 21: Errores del administrador. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Los errores de no registrar adecuadamente las operaciones, sucesos y eventos producidos pueden repercutir en incidentes. De esta manera, se sugiere considerar los errores de monitorización como parte de los riesgos no intencionados.

[NO_INTENCIONADO.3] Errores de monitorización (log)	
Tipos de activos: • (IE) Información Electrónica (IP) Información en Papel – Sobre registro de actividad / registro de errores.	**Dimensiones:** 1. [I] integridad
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	

Ilustración 22: Errores de monitorización. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

El descuido o la negligencia al momento de configurar un dispositivo, puede alterar significativamente la integridad de la información. Es necesario considerar el siguiente aspecto.

[NO_INTENCIONADO.4] Errores de configuración	
Tipos de activos: • (IE) Información Electrónica (IP) Información en Papel	**Dimensiones:** 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

Ilustración 23: Errores de configuración. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

La siguiente tabla hace referencia “Structure” y “Style”, dentro del concepto de las 7S analizado anteriormente.

[NO_INTENCIONADO.5] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad

Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible

Ilustración 24: Deficiencias de la organización. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[NO_INTENCIONADO.6] Alteración accidental de la información	
Tipos de activos: • [IE] Información electrónica • [IP] Información en papel • [SW] Software • [IC] Infraestructura de comunicaciones • [EXTRAIBLE] Soportes de información • [ED] Edificación (Instalaciones)	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

Ilustración 25: Alteración accidental de la información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[NO_INTENCIONADO.7] Destrucción de información	
Tipos de activos: • [IE] Información electrónica • [IP] Información en papel • [SW] Software • [IC] Infraestructura de comunicaciones • [EXTRAIBLE] Soportes de información • [ED] Edificación (Instalaciones)	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

Ilustración 26: Destrucción de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[EL] Errores lógicos

Los errores lógicos son amenazas que afectan directamente al software y la información electrónica. Estos pueden producirse por virus, programas mal compilados o copia ilegal, entre otras posibles alternativas.

[EL.1] Difusión de software dañino	
Tipos de activos: • [SW] software • [IE] Información electrónica	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, malware en general.	

Ilustración 27. Difusión de software dañino. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[EL.2] Copia no controlada de información	
Tipos de activos: • [SW] software • [IE] Información electrónica	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información es copiada accidentalmente sin fines maliciosos y sin el consentimiento de su propietario.	

Ilustración 28. Copia no controlada de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[EL.3] Escapes de información	
Tipos de activos: • Todos	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

Ilustración 29: Escapes de información. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[EC] Errores de Comunicaciones

[EC.1] Errores de [re-]encaminamiento	
Tipos de activos: [SW] (software) • [IC] infraestructura de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no se debía; pudiendo tratarse de mensajes entre personas, entre procesos, entre sistemas o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento o ruteo suponga un error de entrega, acabando la información en manos de quien no se espera.	

Ilustración 30: Errores de re-encaminamiento. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

[EC.2] Errores de secuencia	
Tipos de activos: • [SW] (software) • [IC] infraestructura de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos.	

Ilustración 31: Errores de secuencia. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Paso 4: Análisis de los riesgos

Una vez que el riesgo ha sido identificado, el contexto, causas, factores de contribución y las consecuencias que han sido descritas, se deben considerar las fortalezas y debilidades de

los sistemas y procesos designados para ayudar a controlar el riesgo. Debe conocerse cuales controles ya se encuentran identificados e implementados, si estos son eficaces, si contribuyen en la identificación de algo, si es necesario seguir actuando, o simplemente no colaboran con ninguna acción.

Hay que tomar en cuenta que los controles no siempre requieren algo especial. A veces los controles están presentes como una parte natural de la administración de una situación o área, o se encuentran empotradas en las prácticas diarias de administración.

El proceso para identificar el riesgo se detalla en la sección a continuación.

AR-01.1. Análisis del riesgo

Paso 1: Identificar los controles existentes: Determinar qué controles ya están implementados
para mitigar el impacto del riesgo. Los controles pueden ser fuertes o débiles; pueden ser medible y repetible. Estos pueden incluir legislación, políticas o procedimientos, formación del personal, la separación de funciones, medidas personales, equipos de protección, barreras físicas y estructurales (por ejemplo, la implementación de servidores de seguridad de TI, controles de acceso, o guardias alrededor del centro de procesamiento de datos).

Una vez que los controles se han identificado, y su eficacia ha sido analizada, se deberá realizar una evaluación probabilística de que ocurra el riesgo y las consecuencias si este fuese a ocurrir. Esto produce una exacta, aunque subjetiva, evaluación del nivel de riesgo -o valoración el riesgo-, y ayuda en el siguiente paso para determinar si los riesgos son aceptables o necesitan tratamiento adicional.

Paso 2: Evaluar la probabilidad: Se recomienda que la probabilidad de que ocurra el riesgo sea clasificada en 5 niveles, es decir, descrita como rara, poco probable, posible, probable o casi seguro de que ocurra.

Paso 3: Evaluar la consecuencia: Las consecuencias o potencial impacto de la materialización del evento serán descritas como insignificante, menor, moderada, grave o extrema.

La evaluación de la probabilidad y la consecuencia es sobre todo subjetiva, pero puede ser informada por los datos o información recogida, auditorías, inspecciones, la experiencia personal, el conocimiento corporativo o institucional, memoria de los acontecimientos anteriores, reclamaciones de seguros, encuestas y una gama de otros internos disponibles e información externa.

Paso 4: Valorar el nivel de riesgo: Para la valoración del nivel de riesgo se deberá utilizar la Matriz de Riesgo proporcionada a continuación; esto permitirá evaluar los niveles de probabilidad y consecuencia. La matriz de riesgos ayuda a determinar la calificación del riesgo en cinco niveles: leve, baja, media, alta o extrema. Esta "Matriz de Riesgo" también identifica la acción de gestión requerida para las diferentes clasificaciones de riesgo.

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi certero (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Ilustración 32: Matriz de Riesgo. Fuente: (University of Adelaide, 2015)

Paso 5: Evaluación de los riesgos

Decidir cuales riesgos son aceptables o inaceptables. Lo comprendido sobre el riesgo, utilícelo para tomar decisiones acerca de acciones futuras.

Las decisiones sobre las acciones futuras pueden incluir:

- No emprender o continuar con el evento, actividad, proyecto o iniciativa

- Tratar activamente el riesgo
- Priorizar las acciones necesarias, si el riesgo es complejo y se requiere un tratamiento
- Aceptar el riesgo

Que el riesgo sea aceptable o inaceptable hace referencia a disponerse a tolerar el mismo; es decir, la disposición a asumir el riesgo después de que sea tratado con el fin de lograr los objetivos deseados.

La actitud, el apetito y la tolerancia al riesgo es probable que varíe con el tiempo, a través de la organización en su conjunto y para cada uno de los departamentos, divisiones, subdivisiones y entidades controladas.

Un riesgo puede ser aceptable o tolerable bajo las siguientes circunstancias:

- No se dispone de tratamiento
- Los costos del tratamiento son prohibitivos (particularmente relevante con referencia a riesgos de bajo impacto)
- El nivel de riesgo es bajo y no justifica el uso de los recursos para tratarla
- Las oportunidades involucradas superan significativamente las amenazas

Un riesgo es considerado como aceptable o tolerable si la decisión no ha sido realizada para tratarlo (de acuerdo con el siguiente paso, “Paso 5 'Tratar el riesgo'”).

Es importante recordar que en relación con un riesgo aceptable o tolerable no implica que el riesgo es necesariamente insignificante. Los riesgos que se consideran aceptables o tolerables podrían requerir aun ser supervisados.

Al llevar a cabo una evaluación de riesgos, en general, hay un montón de consecuencias potenciales identificadas. Esto no es necesariamente un problema, ya que un número de estos puede ser abordado por los tratamientos de riesgo, o puede no necesitar ninguna

acción específica. Los tres pasos descritos anteriormente: Identificar el riesgo, Analizar el riesgo y Evaluar el riesgo, forman la fase de evaluación de riesgos en el proceso de gestión de riesgos.

El proceso de la evaluación de riesgos se adapta bien a un enfoque estructurado y sistemático. Para situaciones más complejas, la facilitación de un taller en el que participe personal de la empresa con diferentes puntos de vista, a menudo es útil; y la incorporación de un facilitador con experiencia para dirigir la discusión, puede ayudar a proporcionar otra perspectiva objetiva.

Paso 6: Tratamiento de los riesgos

De los resultados obtenidos en la matriz de Riesgo, se deberán considerar los siguientes niveles de aceptación de riesgo:

Niveles de riesgo - Acción de gestión requerida	
Riesgo extremo (E)	Requiere respuesta y atención inmediata.
Riesgo alto (A)	Debe otorgársele la atención apropiada.
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora.

Ilustración 33: Acción de gestión requerida. Fuente (University of Adelaide, 2015)

Considerando las buenas prácticas expuestas por (Ministerio de Hacienda y Administraciones Públicas de España, 2012), (Microsoft, 2006), (University of Adelaide, 2015), (Cornell University Law School, 2016), (Yazar, 2002), (Vásquez & López, 2016) , y (Crespo & Cordero, 2016); el proceso para el tratamiento de riesgo puede ser definido en los siguientes pasos:

Paso 1: Decidir si es necesario un tratamiento específico o si el riesgo puede ser tratado adecuadamente durante el curso de procedimientos normalizados de gestión y actividades de tratamiento específico; es decir, integrar el tratamiento o procesos en las prácticas del día a día. En la evaluación de los tratamientos que podrían ser implementados, es importante considerar aspectos en los cuales las prácticas estándar sirven como control, o maneras en las que esas prácticas estándar podrían ser modificadas para controlar adecuadamente el riesgo.

Paso 2: Trabajar en lo que se quiere como deseable para el tratamiento de riesgo: Determinar cuál es el objetivo del tratamiento de ese riesgo en particular para evitarlo completamente, para reducirlo, para transferirlo o simplemente aceptar el nivel de riesgo existente. El tipo de riesgo elegido puede depender de la naturaleza del mismo y su tolerancia.

Paso 3: Identificar y diseñar una opción preferente de tratamiento, una vez que el objetivo del tratamiento ha sido conocido.

- Si la meta es reducir la probabilidad o posibilidad del riesgo, entonces se debe ajustar a lo que sucedería o debería planificarse: Alterar con éxito el enfoque dependerá de la identificación de las causas de la amenaza y la relación causal entre ella y su impacto; ambos de los cuales deberían haber sido identificados en la fase de evaluación de riesgos.
- De no ser posible el cambio de la aproximación de la actividad, entonces podría ser posible tomar otra acción de intervención para mitigar la ocurrencia del evento, o reducir la probabilidad de la treta.
- El comprender la naturaleza del evento de riesgo y la forma de como ésta se produce, puede resultar de gran ventaja al momento de identificar de forma más sencilla cualquiera de las acciones de intervención posibles que permitan reducir el riesgo.

- Si la meta es reducir la consecuencia o el impacto del riesgo, los planes de contingencia serán requeridos para responder al tratamiento si el evento ocurre. Esta planeación puede ser llevada a cabo en combinación con otros controles; incluso si se han tomado medidas para reducir al mínimo la probabilidad del riesgo, no debe descartarse la posibilidad de incluir un plan en marcha para la mitigación de las consecuencias si es que el evento llegara a producirse.
- Si el objetivo es compartir el riesgo, entonces la participación de un tercero, tal como un asegurador o contratista, puede ayudar. El riesgo puede ser compartido mediante un contrato de común acuerdo, y en una variedad de formas que satisfagan las necesidades de todas las partes. Dichos acuerdos deben ser registrados formalmente, ya sea a través de un contrato, de un acuerdo o mediante una carta. Compartir el riesgo no libera de obligaciones y no evita asumir las consecuencias del daño o de algo que podría salir mal.
- Si el riesgo es tan importante que el objetivo es eliminar o evitarlo por completo, entonces las alternativas se limitan a cambiar el proyecto materialmente, a elegir enfoques o procesos alternativos para hacer el riesgo irrelevante o terminar en el abandono de la actividad o programa. Se debe saber que, generalmente, el riesgo no puede ser eliminado por completo y que su equilibrio es una parte importante del ejercicio del aseguramiento de los mismos.
- A veces, la decisión es aceptar o tolerar el riesgo, debido a la baja probabilidad o consecuencias menores del evento de riesgo, o el hecho de que el costo de controlarlo es injustificadamente alto o que la oportunidad sea superior al riesgo. Sin embargo, estas decisiones para aceptar el riesgo deben ser cuidadosamente documentadas, de manera que estas queden como evidencias o futuras referencias.

Paso 4: Evaluar las opciones de tratamiento y su viabilidad en relación con la tolerancia al riesgo. Puede realizar el siguiente cuestionamiento: ¿Los controles seleccionados parecen tener el efecto de tratamiento deseado (es decir, van a detener o reducir lo que se supone se quiere detener o reducir)?

- ¿Pueden los controles de desencadenar cualquier otro riesgo? Por ejemplo, un sistema de aspersores instalado para contrarrestar riesgo de incendio puede causar daños por agua, presentando un riesgo diferente a lo que estuvo inicialmente considerado.
- ¿Los controles ofrecen un beneficio? ¿El costo de implementar el control supera el costo que se derivaría si el evento ocurre sin el control sugerido? En general, ¿el costo de la implementación del control es razonable para este riesgo?

El proceso del tratamiento de riesgo es cíclico, decidiendo si los niveles de riesgo residual son tolerables, y asegurando la efectividad del tratamiento caso por caso.

Paso 5: Documentar el plan de tratamiento de riesgo: Una vez que las opciones del tratamiento han sido identificadas, un plan de tratamiento deberá ser preparado. Este plan deberá identificar los roles, responsabilidades y cronograma para su implementación, el presupuesto, indicadores de desempeño y la revisión de los procesos que fuesen apropiados. La revisión de los mismos deberá permitir el monitoreo del progreso de los tratamientos frente a la implementación de hitos críticos.

Paso 6: Aplicar tratamientos acordados. Una vez que todas las opciones que requieren autorización para la dotación de recursos, la financiación u otras medidas han sido aprobadas, los tratamientos deben ser aplicados por quienes los hayan identificado, a manera de que sea de sean los responsables en hacerlo. La persona que tenga asignada la responsabilidad principal del riesgo, será la responsable en última instancia del tratamiento del mismo.

Paso 7: Una vez que el riesgo ha sido tratado, se deberá evaluar el nivel de riesgo residual. Incluso cuando el riesgo ha sido tratado y los controles están en su lugar, el riesgo puede no ser eliminado del todo. El nivel de riesgo residual se refiere a la probabilidad y la consecuencia de que el riesgo ocurra después de que el mismo ha sido tratado. Por ejemplo, puede darse la probabilidad de que un equipo se infecte con virus, aun contando con un antivirus instalado.

Una vez implementado, las alternativas de tratamiento proporcionarán o modificarán los controles. La calificación de riesgo residual es generalmente inferior al valor nominal original de los riesgos, de lo contrario los controles seleccionados no fueron eficaces.

Consideración importante: El riesgo residual, al ser latente, debe ser monitoreado, documentado y constantemente evaluado.

Paso 7: Identificación de contramedidas

Según (Ministerio de Hacienda y Administraciones Públicas de España, 2012), las contramedidas permiten mitigar las amenazas y su materialización. Hay que tener claro que muchas de ellas, en especial las técnicas, suelen variar con el avance tecnológico, ya que:

- Aparecen tecnologías nuevas
- Van desapareciendo tecnologías antiguas
- Cambian los [tipos de] activos a considerar
- Evolucionan las posibilidades de los atacantes o
- Evoluciona el catálogo de contramedidas disponibles.

Para seleccionar las contramedidas que brindarán protección a los activos organizacionales, se deberá considerar, primeramente, los elementos de protección actual establecidos, y luego los posibles elementos de control que podrán ser implementados. En base a los controles que sugiere la norma UNE-ISO/IEC 27001:2013 que son aplicables en el contexto de las capacidades de una MPYME, una organización de este sector deberá considerar los siguientes elementos de salvaguardas:

TIPO DE PROTECCIÓN	
PGeneral	Protección de tipo general
PInfo	Protección de Información Electrónica y de Papel
PSW	Protección de software
PHW	Protección del hardware

PIC	Protección de la Infraestructura de Comunicaciones
PSF	Seguridad Física, relativa a edificaciones e instalaciones.
PRRHH	Relativas a los Recursos Humanos

Ilustración 34: Tipos de protección. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Protecciones de tipo general

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles de tipo general:

- Protección de acceso a lugares sensibles
- Cámaras de monitoreo y vigilancia
- Extintores contra incendio
- Sensores de humedad, calor, humo
- Aspersores
- Antivirus
- Antispyware
- Procedimientos para la gestión de vulnerabilidades
- Segregación de tareas
- Herramientas para identificación y autenticación
- Herramientas para monitorización de tráfico
- Herramientas para el análisis de logs
- Herramientas para el análisis de actualizaciones y parches de sistemas operativos
- Defensa en profundidad
- Procedimientos para aseguramiento de la disponibilidad

Protección de Información Electrónica y de Papel

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para Información electrónica y de Papel:

- Copias de seguridad de los datos
- Cifrado de información sensible
- Procedimientos para aseguramiento de la calidad
- Gestión de llaves y certificados digitales

Protección de software

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para software:

- Copias de seguridad
- Procedimientos para puesta en producción
- Procedimientos para modificación de software
- Procedimientos para baja segura de software

Protección del hardware

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para hardware:

- Protección de hardware (en ambientes de desarrollo, pre producción y producción)
- Procedimientos para la gestión de la disponibilidad
- Procedimientos para la correcta operación
- Procedimientos para la baja / reemplazo
- Procedimientos para el manejo seguro de computación móvil

Protección de la Infraestructura de Comunicaciones

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para Infraestructura de comunicaciones:

- Aseguramiento de la disponibilidad
- Procedimientos para cambios (actualizaciones y mantenimiento)
- Consideraciones para uso de Internet
- Consideraciones para el uso de telefonía móvil
- Aseguramiento del canal
- Aseguramiento de entrada de servicio

Seguridad Física, relativa a edificaciones e instalaciones.

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para seguridad física:

- Protección de acceso a lugares sensibles
- Cámaras de monitoreo y vigilancia
- Extintores contra incendio
- Sensores de humedad, calor, humo
- Aspersores
- Políticas de uso de infraestructura
- Políticas ante emergencias

Relativas a los Recursos Humanos

Al menos los siguientes elementos deberán ser considerados en las protecciones o controles para Recursos Humanos:

- Gestión del personal
- Formación y concienciación
- Aseguramiento de la disponibilidad

Paso 8: Monitoreo y revisión

Esta etapa hace referencia a la supervisión de cambios en la fuente y el contexto de los riesgos, la tolerancia a ciertos riesgos y la adecuación de los controles. Busca garantizar que los procesos se encuentran implementados para revisar, evaluar e informar sobre los riesgos con regularidad.

De esta manera, para asegurar una revisión estructurada y la notificación periódica en cada una de las áreas, será importante considerar procesos que permitan identificarlos. Dada la naturaleza diversa y dinámica del entorno de la MPYME ecuatoriana, es importante estar alerta a los riesgos emergentes, así como el seguimiento de los riesgos conocidos.

Importante: El monitoreo y la revisión es parte de la planificación del proceso de gestión de riesgos.

El proceso de monitoreo y revisión se resumen a continuación:

Paso 1: Monitoreo continuo: Una vez que los riesgos han sido identificados, almacenados, analizados y luego de haber acordado las contramedidas a ser implementadas, un sistema y política de monitoreo y reporte debe ser establecido para proveer la seguridad y garantía de que el tratamiento del riesgo será efectivo y que ayudará a contrarrestar la amenaza. Algunos tratamientos de riesgo provienen de las prácticas y métodos diarios de trabajo.

La frecuencia de la revisión depende del nivel de riesgo identificado, la fortaleza de los controles y la habilidad para tratarlos. Cada uno de los miembros de la organización deben cumplir con un rol de monitoreo constante de los riesgos conocidos y emergentes, y regularmente deberán verificar y asegurar que los controles y contramedidas están funcionando adecuadamente.

El comité de riesgo deberá velar por el cumplimiento de las políticas y procedimientos establecidos, por cada una de las áreas de negocio. Siempre que sea posible, la gestión de riesgos deber ser un aspecto a tratarse en cualquier reunión.

Auditoría interna deberá considerar en sus planes de auditoría un programa que incluya la revisión a los sistemas, políticas y procedimientos de seguridad y su cumplimiento.

Paso 2: Reportar de manera formal: Es una actividad importante, ya que es capaz de demostrar la eficiencia y eficacia del programa de gestión de riesgos. La organización se somete a la obligación de informar a cada uno de los interesados (stakeholders) de manera oportuna y transparente.

El proceso de reporte puede incluir:

- Reportes de comité de gestión de riesgos semanales o quincenales.
- Reportes semestrales de riesgos extremos y de nivel alto a la alta gerencia, dirección o propietario.

Paso 3: Se deberá registrar, al menos:

- Una descripción del riesgo (en base al contexto)
- Causas o factores contribuyentes
- Consecuencias o impactos del riesgo, actuales o potenciales
- Controles actuales que ayudan a mitigar el riesgo
- Una evaluación de la probabilidad y la consecuencia basada en el control actual, para establecer el nivel de prioridad de cada riesgo.
- Acciones futuras o tratamientos necesarios para direccionar el riesgo.
- Cualquier actualización a ser implementada para el tratamiento de riesgo
- Resultados del monitoreo y revisión, incluyendo la efectividad de los controles.

Paso 9: Comunicar y consultar

La comunicación efectiva y la consulta son esenciales para asegurar que los responsables de la implementación de la gestión de riesgos, y los que tienen un interés personal, puedan comprender la base sobre la que se toman las decisiones y las razones por las cuales se seleccionan las opciones de tratamiento particulares.

Los métodos de comunicación y consulta podrían incluir:

- Reuniones
- Reportes
- Sistemas de comunicación en línea
- Talleres de inducción y capacitación a los empleados
- Noticias
- Grupos focales

El equipo encargado de la comunicación tendrá como objetivos:

- Ayudar a establecer el contexto de forma apropiada
- Asegurar los intereses de todos los interesados sean conocidos y considerados
- Asegurar que los riesgos son adecuadamente identificados
- Brindar ideas en común sobre áreas de experiencia cuando se asegure o analice el riesgo
- Colaborar con la asignación y soporte del plan de tratamiento de riesgos
- Comunicar las mejoras logradas en los procesos asociados con el riesgo.

Parte D: Recursos

Matriz para la identificación de activos de información

Las columnas C, D, I, hacen referencia a Confidencialidad, Disponibilidad e Integridad, respectivamente.

Hardware

id_Activo	incremental	Tipo	Numero Serie	Mac	Fecha compra	Proveedor	Garantía	C	D	I	Valoración

Ilustración 35: Matriz de inventario de activos de hardware. Fuente: Autoría propia

Software

Id_Activo	incremental	Descripción	Versión	Numero Serie	Clave Activación	Fecha Compra	Actualización	Proveedor	C	D	I	Valoración

Ilustración 36: Matriz de inventario de activos de software. Fuente: Autoría propia

Información Electrónica

Id_Activo	Incremental	Tipo	Fecha creación	Tamaño	Permisos	Ubicación	Nombre	Fecha modificación	Creador	C	D	I	Valoración

Ilustración 37: Matriz de inventario de activos de Información electrónica. Fuente: Autoría propia

Información Electrónica

Id_Activo	Incremental	Tipo	Fecha creación	Ubicación	Nombre	Fecha modificación	Creador	C	D	I	Valoración

Ilustración 38: Matriz de inventario de activos de Información en papel. Fuente: Autoría propia

Infraestructura de comunicaciones

Id_Activo	Incremental	Tipo	Categoría	Nombre	Proveedor	Fecha_contrato	C	D	I	**Valoración**

Ilustración 39: Matriz de inventario de activos de Infraestructura de comunicaciones. Fuente: Autoría propia

Medios de almacenamiento extraíbles

Id_Activo	Incremental	tipo	Capacidad	mac	Fec_adquisición	Proveedor	Garantía	C	D	I	**Valoración**

Ilustración 40: Matriz de inventario de activos de Medios de almacenamiento extraíbles. Fuente: Autoría propia

Recursos humanos

ID_Activo	Incremental	Nombre	Apellido	Cargo	Género	FECHA DE INGRESO	FECHA DE SALIDA	C	D	I	**Valoración**

Ilustración 41: Matriz de inventario de activos Recursos Humanos. Fuente: Autoría propia

Edificaciones / Instalaciones

ID_Activo	Incremental	Descripción	Ubicación	C	I	D	**Valoración**

Ilustración 42: Matriz de inventario de activos de Edificaciones / Instalaciones. Fuente: Autoría propia

Matriz para el registro de riesgos

[COD RIESGO] RIESGO	
Activos afectados:	**Dimensiones:** [D] disponibilidad [I] integridad [C] confidencialidad
Descripción:	

Ilustración 43: Matriz para el registro de riesgos. Fuente: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Registro y cálculo de riesgos

	Valor					Impacto			Degradación			Riesgo Acumulado			Riesgo Residual		
ACTIVO	C	D	I	TOTAL	Frecuencia %	C	D	I	C	D	I	C	D	I	C	D	I
ID Activo				MAX		0%	0%	0%	-	-	-						
Amenaza 1																	
Amenaza 2																	
Amenaza 3																	
.																	
.																	
Amenaza N																	

Ilustración 44: Registro y cálculo de riesgos. Fuente: (27001 Academy, 2015)

Matriz para el manejo de riesgos

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi cierto (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Ilustración 45: Matriz de Riesgo. Fuente: (University of Adelaide, 2015)

De acuerdo a lo mencionado en los procesos anteriores, para la interpretación de los valores, se deben considerar los siguientes niveles de riesgo:

Niveles de riesgo - Acción de gestión requerida	
Riesgo extremo (E)	Requiere respuesta y atención inmediata.
Riesgo alto (A)	Debe otorgársele la atención apropiada.
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora.

Ilustración 46: Acción de gestión requerida. Fuente (University of Adelaide, 2015)

Cuestionario sobre aplicabilidad de la metodología

Cuestionario sobre aplicabilidad de la metodología
(Basado en el estándar ISO27001)

Nro.	Asunto	Sí	No
	Políticas de Seguridad de la Información		
1	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?		
	En caso de existir el documento:		
2	¿Considera Usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		
3	¿El documento de seguridad es revisado periódicamente y en caso de ocurrencia de eventos significativos?		
	Seguridad Organizacional		
4	¿Existe un comité de gestión de seguridad que proponga o de soporte a las iniciativas de seguridad?		
5	¿Existe algún tipo de coordinación de seguridad de la información desde donde se coordine la implementación de controles a lo largo de todos los componentes de la organización?		
6	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?		
7	¿Existe el soporte y la asistencia de un servicio de consultoría especializado en seguridad de la información?		
8	¿Están establecidos contactos y acuerdos de cooperación con organizaciones para el manejo de asuntos de seguridad?		

9	¿Se realizan auditorias de seguridad independientes a la implantación de las políticas de seguridad de la información de la organización?		
10	¿Se establecen contratos formales de seguridad cuando recursos de tecnologías de información de su organización serán accedidos y/o manejados por terceros?		
	Clasificación y control de activos		
11	¿Se mantiene un inventario de todos los activos sensibles de cada sistema de información de la organización?		
12	¿Existen esquemas o directrices para la clasificación de la información de la organización de acuerdo al grado de protección que deban recibir?		
13	¿Están definidos los controles de protección asociados al grado de protección que deba recibir cada activo de información?		
14	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?		
	Seguridad y personal		
15	¿Incluyen los perfiles de trabajo o cargo responsabilidades en el área de seguridad?		
16	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?		
17	¿Se educa y entrena a los empleados adecuadamente en las políticas y procedimientos de seguridad de la organización?		
18	¿Conocen los empleados los procedimientos para reportar amenazas, riesgos, sospechas u ocurrencias de: incidentes de seguridad, debilidades en sistemas o servicios e incorrecto funcionamiento de aplicaciones/software?		
19	¿Están definidos los procesos disciplinarios para sancionar a aquellos empleados que incurran en violaciones a las políticas y procedimientos de seguridad de la información de la organización?		
	Seguridad física y ambiental		
20	¿Las áreas con sistemas basados en tecnologías de la información están protegidas físicamente a través de un perímetro de seguridad?		
21	¿Existen controles de entrada a las áreas con activos de información sensibles?		

Nro.	Asunto	Sí	No
22	¿Son esos controles de entrada efectivos, es decir, sólo permiten el acceso a personal autorizado?		
23	¿Las oficinas, cuartos y salas contentivas de activos de información con requerimientos de seguridad especiales se encuentran en áreas creadas para ese fin?		
24	¿Existen normas, procedimientos y mecanismos de control adicionales para trabajar en las áreas seguras? ¿Cuáles son?		
25	¿Están las áreas de carga y despacho de la organización aisladas de las zonas donde se localizan los activos y sistemas basados en tecnologías de la información?		
26	¿Está el equipamiento en tecnologías de la información adecuadamente protegido para reducir riesgos o la exposición a amenazas ambientales o de acceso no autorizado?		
27	¿Está el equipamiento protegido contra fallas o anomalías eléctricas?		
28	¿Está el cableado eléctrico y de telecomunicaciones asociado al transporte de datos o al soporte de los sistemas basados en tecnologías de información protegido contra intercepciones o daño físico?		
29	¿Los equipos que conforman los servicios basados en tecnologías de la información son sometidos a las labores de mantenimiento indicadas por los fabricantes, así como en el período de tiempo especificado?		
30	¿Se autoriza y controla el uso de equipos para procesar información que no cumplan con		

	las directrices de seguridad de la organización? ¿Quién lo autoriza?		
31	¿Se realiza algún tratamiento a la información almacenada en un equipo previo a su desincorporación o reúso? ¿Qué se hace?		
32	¿Implementa su organización una política de escritorios y pantallas limpias?		
33	¿Existen controles que sólo permitan el retiro de: equipamiento, software e información perteneciente o en custodia por la organización con la autorización de la gerencia?		
	Gestión de la operación y las comunicaciones		
34	¿Están documentados los procedimientos de seguridad contemplados en la política de seguridad de la organización?		
35	¿Están establecidos los procedimientos y roles para el manejo de incidentes de seguridad?		
36	¿Los ambientes de prueba y desarrollo de sistemas basados en tecnologías de la información están separados del ambiente operativo?		
37	¿Existen mecanismos para monitorear el uso de los sistemas de la organización? (Como soporte para planificar crecimiento y evitar el colapso de la capacidad de procesamiento de información de la organización)		
38	¿Se definen criterios y planes de prueba para aceptar el uso de nuevos sistemas de información (o nuevas versiones/actualizaciones)?		
39	¿Se educa y concientiza a los usuarios en las medidas que deben tomar para evitar ser víctimas de software malicioso?		
40	¿Están implantadas medidas efectivas para detectar y prevenir contra la presencia de software malicioso?		
41	¿Existen políticas y procedimientos para la ejecución de respaldos y su verificación?		
42	¿Existen registros de las actividades o trabajos que se realizan o intentan realizarse sobre los sistemas basados en TI de la organización?		
43	¿Están implantados mecanismos para proteger la plataforma de red de la organización y la información que pasa a través de ella?		
44	¿Los dispositivos o medios de almacenamiento de información removibles como cintas, discos, información impresa, etc., tienen definido normas o controles que regulen su manejo (protección) y desecho?		
45	¿Se protege la documentación de los sistemas de información de la organización? ¿Cómo?		
46	¿Existen reglas y procedimientos que gobiernen y controlen el intercambio de información y programas entre organizaciones ?		

Nro.	Asunto	Sí	No
	Control de acceso		
47	¿Posee la organización una política de control de acceso?		
48	¿Existen diferentes niveles de acceso o privilegios para acceder a la información? ¿Cómo se asignan?		
49	¿Existen procedimientos de auditoria para revisar y corregir los derechos de acceso de los usuarios de los sistemas de la organización?		
50	¿Los usuarios son educados sobre sus responsabilidades o rutinas en el manejo de sus mecanismos de acceso a los sistemas?		
51	¿Existe una política de uso de los servicios de la red?		
52	¿Se restringe o controla el acceso a los servidores de la red? ¿Cómo?		
53	¿La red está segregada siguiendo algún criterio? ¿Cuál o cuáles?		
54	¿Existen mecanismos de control de tráfico para evitar que flujos de datos y conexiones de otros nodos violenten la política de control de acceso?		

55	¿Los atributos de seguridad que poseen los servicios de red que utiliza la organización son adecuados?		
56	¿Se utilizan mecanismos y herramientas de monitoreo para detectar usos irregulares de la red?		
57	¿Todos los relojes de los sistemas en la red están sincronizados?		
58	¿Se controla el acceso a la red y sistemas de la organización desde facilidades de computación móvil y tele-trabajo? ¿Cómo es controlado?		
	Desarrollo y mantenimiento de sistemas		
59	¿Son los requerimientos de seguridad incluidos en el desarrollo de nuevos sistemas o en las mejoras a los ya existentes?		
60	¿Poseen los sistemas mecanismos de seguridad para prevenir su mal uso?		
61	¿Es el proceso de desarrollo de software conducido de una manera segura y metodológica?		
62	¿La implementación de cambios es realizada utilizando procedimientos formales de control de cambio?		
	Gestión de la continuidad del negocio		
63	¿Posee la organización un proceso de gestión para desarrollar y mantener planes para la continuidad del negocio ante los efectos de fallas mayores o desastres?		
64	¿Son los planes de continuidad del negocio constantemente revisados y corregidos para asegurar su efectividad?		
	Cumplimiento con el marco jurídico		
65	¿Tienen los sistemas de información definidos y documentados todos los requerimientos legales relevantes y las normas para asegurar su cumplimiento?		
66	¿Están establecidas directrices para la retención, almacenamiento, manejo y desecho de registros e información de la organización?		
67	¿Existen directrices a todo nivel (gerencia, usuarios y proveedores de servicio) sobre las responsabilidades y procedimientos a seguir para garantizar la protección e intimidad de la información de los clientes?		
68	¿Existen medidas para prevenir del uso de las facilidades de procesamiento de información en propósitos diferentes a los del negocio?		
69	¿Están los controles criptográficos adaptados a las normas que regulan su funcionamiento dentro de Ecuador?		
70	¿Las normas y controles adoptados para recolectar evidencia para soportar una acción legal están acordes con las leyes pertinentes?		
71	¿Se realizan revisiones programadas a todos los entes involucrados con el negocio para asegurar que cumplen con las políticas y estándares de seguridad de la organización?		

Ilustración 47: Cuestionario sobre aplicabilidad de la metodología. Fuente:ISO 27001

Aspectos considerados en la construcción de ECU@Risk

Para la construcción de la metodología ECU@Risk, se han adoptado los aspectos más relevantes de las metodologías estudiadas: CRAMM, OCTAVE-S, Microsoft Risk Management y Magerit V3; además de las normativas ISO 27001, ISO 27002, ISO 27005 e ISO 31000. La tabla que se presenta a continuación resume los aspectos considerados para cada una de las etapas que contempla la metodología.

Proceso	Aspecto	Metodología modelo
Parte A: La introducción al manejo de riesgo		
Introducción a la gestión de riesgo	Conceptos introductorios a la gestión de Riesgo	ISO 31000
Parte B: El marco de gestión de riesgo		
Identificación y definición de roles y funciones	Requerimientos, roles y funciones del personal encargado de la gestión de riesgo	ISO 31000 COBIT 5, COSO III, Normativa Vigente de la República del Ecuador, 7S McKinsey, Cadena de Valor de Porter, Modelo PESTEL, Modelo FODA, Metodología para la gestión de procesos de Servicio, Modelo Servqual

Parte C: El proceso de gestión de riesgo		
Paso 1: Establecer el contexto	Establecer el contexto en el que se desarrolla el negocio e involucra a la información	Microsoft Risk Management, Octave-S, Cramm, ISO 27001, ISO 27002, Normativa Vigente de la República del Ecuador,
Paso 2: Identificar los activos de información	Adopta la mayoría de los grupos de clasificación para los activos de información Además, adopta los criterios para determinar las dimensiones de valoración, y además razonamientos para la valoración de los activos	Magerit V3, ISO 27001, ISO 27002
	Registro de los activos de información	Microsoft Risk Management ISO 27001, ISO 27002
	Escala de Criterios de valoración	Magerit V3 ISO 27001, ISO 27002
Paso 3: Identificación de los riesgos	Identificación de las amenazas. Adopta el modelo de clasificación de los grupos de riesgo.	Magerit V3, Octave-S ISO 27001, ISO 27002
Paso 4: Analizar los riesgos	Identificar los controles existentes	Magerit V3, CRAMM, Octave-S ISO 27001, ISO 27002, ISO 27005

	Evaluar la probabilidad	Microsoft Risk, ISO 27005, ISO 31000
	Evaluar la consecuencia	ISO 27005, ISO 31000
	Valorar el nivel de riesgo	Magerit V3, Octave-S, ISO 27005, ISO 31000
Paso 5: Evaluación del riesgo	Identificar los aspectos que permiten evaluar el riesgo	Microsoft Risk, Magerit V3, ISO 27005, ISO 31000
Paso 6: Tratamiento de los riesgos	Identificar las mejores prácticas para el tratamiento del riesgo	Microsoft Risk, Magerit V3, ISO 27005, ISO 31000
Paso 7: Identificación de contramedidas	Evaluar alternativas de protección de activos de información	Magerit V3, COBIT 5, ISO 27001, ISO 27002, ISO 27005, ISO 31000
Paso 8: Monitoreo y revisión	Identifica el procedimiento para monitoreo y revisión como parte de la planificación del proceso de gestión de riesgos.	ISO 27005, ISO 31000, COBIT 5, COSO III
	Establecer parámetros de reporte de incidentes	ISO 27005, ISO 31000, COBIT 5, COSO III, Microsoft Risk
Paso 9: Comunicar y consultar	Identifica el procedimiento más adecuado para comunicar y consultar las contramedidas y los temas de riesgo dentro de la organización	ISO 27005, ISO 31000, COBIT 5, COSO III

Conclusiones

Las amenazas están latentes, todo sistema de información es vulnerable y la probabilidad de riesgo es inminente dependiendo de su contexto. Sin embargo, pueden presentarse situaciones no controladas o inesperadas; dejando en claro que el riesgo no puede ser mitigado en su totalidad, pero si puede ser controlado.

Tras la tragedia producida el 16 de abril del 2016 por el terremoto, cuyo epicentro estuvo al norte de la provincia de Manabí, en la costa ecuatoriana, refleja lo mencionado anteriormente; pues aparentemente la mayoría de negocios no contaban con un plan de continuidad, retomando las operaciones luego de un tiempo considerable. Es interesante cuestionarse ¿Qué pasó con la información de inventarios o de facturación que mantenían esas MPYMES? ¿Cómo saben ahora cuáles son sus deudores y cuál es el valor a cancelar a sus acreedores? Es probable que los activos físicos se hayan visto afectados, pero en sí la información debería ser recuperada si se contaba con un adecuado plan de contingencia y procedimientos claros para la gestión de riesgos. Está claro que las empresas del sector MPYME no están preparadas para enfrentar los riesgos de manera formal, esto es, los riesgos son manejados a un nivel AdHoc o simplemente los maneja como respuesta a un incidente.

Dimitrik Bestuzhev, especialista de Kaspersky y expositor del 1er Seminario de Ciberseguridad y Ciberdefensa llevado a cabo en la Universidad del Azuay en octubre del 2015, mencionó que el Ecuador mantiene un alto nivel de riesgo en cuanto a información se trata. La iniciativa tomada por el administrador de la página web, o del técnico de soporte institucional no es suficiente; debido a ello, los altos mandos de cualquier institución, ya sean públicas, privadas o sin fines de lucro, deben estar conscientes de los arduos problemas que puede acarrear las organizaciones cuando una amenaza es materializada.

De la entrevista realizada a los gerentes generales y responsables de TI en 50 organizaciones del sector MPYME ecuatoriano, se revela que, si bien se realizan copias de seguridad de la información, esta es mantenida en los mismos servidores de la empresa; sin

embargo, estas actividades no son formales, no cuentan con evidencia de hacerlas de forma periódica y, peor aún, las copias nunca han sido probadas. Tampoco tienen delimitadas las áreas sensibles del negocio. Así, por ejemplo, algunas organizaciones tienen el servidor principal en un espacio asignado para la cafetería, donde el equipo está conectado al mismo tomacorriente que la cafetera. Esto demuestra desconocimiento de las operaciones sobre el sistema informático, del valor monetario de la información y del riesgo que podría presentarse en la organización si la información es extraviada, no recuperada o alterada sin consentimiento.

Consecuentemente, la investigación realizada permite afirmar que las empresas del sector MPYME no cuentan con una metodología clara de actividades a realizar para la gestión de los activos de información y los riesgos que pudiesen presentarse, así como tampoco tienen un plan de contingencia para recuperación ante un desastre. Tratar de que una MPYME adopte una metodología compleja como COBIT o COSO, o cumplir con todos los requisitos de una normativa ISO podría resultar inalcanzable tanto por esfuerzos logísticos como económicos.

ECU@Risk, es una metodología fruto del análisis de otras múltiples utilizadas a nivel internacional para la gestión de riesgos, las mismas que reflejan aspectos positivos y consideraciones especiales de cada una de las normativas ISO utilizadas en la gestión de riesgo y la seguridad de la información.

Para escribir esta metodología, se fundamentaron algunos de sus procedimientos en base al análisis de las metodologías internacionales CRAMM, Magerit, Microsoft Risk Management, y Octave-S. Una vez estudiadas todas ellas, se ha podido concluir que, en un primer acercamiento, la metodología más sencilla de manejar es la de Microsoft, sin embargo, ésta se encuentra más orientada a la seguridad informática, pues el nivel y profundidad con la que clasifica los activos de información es bastante elemental.

ECU@Risk, al igual que la guía Microsoft Risk Management, tiene la ventaja de que, para un entorno ecuatoriano, se encuentra escrita en lenguaje español. Coincidiendo con la

opinión de (Vásquez & López, 2016) sobre Microsoft Risk Management en cuanto a ser una alternativa viable desarrollada por especialistas computacionales que buscaban crear conciencia sobre los posibles riesgos informáticos; ECU@Risk también es una metodología técnica que considera la perspectiva de los clientes, los entornos MPYMEs ecuatorianos y sus necesidades, la valoración cuantitativa y cualitativa de los activos de información, así como el planteamiento de un esquema de investigación y gestión de riesgos que será ejecutado en cada una de las organizaciones.

Esta metodología proporciona un esquema de análisis en el que se consideran herramientas propias de la gestión empresarial, tales como la matriz de análisis PESTEL, la misma que brinda directrices para analizar macro ambiente en el que se desenvuelve la organización. También considera procedimientos basados en las 7S de McKinsey, los cuales permiten identificar el comportamiento organizacional y hacer un análisis interno, que, para este caso, fue de interés el comportamiento humano en cuanto a un estilo de dirección particular y sometido a cierto tipo de sistemas conocidos como políticas y procedimientos. Se completa el conjunto de herramientas con la inclusión de la matriz FODA, sabiendo que esta es una herramienta de gestión que puede alertar sobre amenazas, las mismas que al final pueden materializarse.

Al igual que las metodologías internacionales, ECU@Risk propone una plantilla que servirá para la recolección y valoración de cada uno de los datos relevantes que componen un activo de información, sabiendo que estas ayudarán a inventariarlos, estudiarlos, administrarlos y gestionarlos.

En su alineación con marcos metodológicos más completos, conocidos también como metodologías de Gobierno de TI, específicamente COBIT, ECU@Risk analiza aspectos relacionados con las estructuras organizativas, donde para cada empresa tendrá definida una estructura variada; y que, en función de su composición y ámbito de decisiones, las mismas podrán ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno de una

organización trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno (ISACA, 2012).

ECU@Risk considera como elemento importante el talento humano y sus habilidades. Para ISACA, "*las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas*". En su catálogo de herramientas incluidas, se ha considerado a STYLE, una de las 7 S de McKinsey, que es la que hace referencia al estilo y la habilidad gerencial o de liderazgo, quedando claro que esta es fundamental para miembros que conforman tanto el órgano de gobierno como el de gestión, es comprender sus propias actividades además de saber diferenciarlas.

Se han considerado las plantillas y matrices contenidas en Magerit V3 en su catálogo de elementos, debido a que sugieren elementos de identificación que podrían contemplados en cada una de las fases de identificación de riesgos. La guía es muy clara y también se encuentra escrita en idioma español, y su última actualización es en el 2012. Además, ofrece la sintaxis XML para el intercambio de información entre plataformas. ECU@Risk ha considerado estas plantillas y matrices adaptándolas al entorno local.

Por otro lado, CRAMM, es una metodología que fue actualizada por última vez a finales de la primera década del siglo XXI, no es de acceso gratuito y está disponible únicamente en idioma inglés; sin embargo, contiene una guía muy detallada sobre planificación, procesos y elementos a considerar en la identificación de activos, amenazas y riesgos. La desventaja es que, al ser demasiado extensa, se enfoca más a las grandes empresas, además de dejar de lado el principio de no repudio; por cuanto no sería aplicable directamente a una MPYME. Está basada en el contexto británico, por cuando quedaría muy lejos de la realidad ecuatoriana.

De cualquier forma, para todas las metodologías estudiadas, la información de cada uno de los activos, amenazas y riesgos, es recolectada en plantillas y matrices. Risk y Octave-S han proporcionado recomendaciones para la planificación de reuniones futuras, en donde el reto consiste el diseño de un efectivo plan de políticas de seguridad, cuyo objetivo es

permitir mitigar los riesgos que podrían presentarse, afectando a cada una de las dimensiones valoradas de los activos de información.

Risk, al igual que Octave-S, sugiere que las reuniones deben estar basadas en debates direccionados, considerando actividades de control y monitoreo efectivo y permanente del sistema informático, y que finalizará con evaluaciones dadas por cada uno de los participantes. En cada una de estas, deberá asistir todo el personal que sea responsable de la información (dueño de información) de una empresa, con el objetivo de identificar aspectos de riesgo operativo y tecnológico. Además, consideran que es importante el manejo de terminologías desconocidas o aspectos que no forman parte de la organización mediante un lenguaje más general y asimilable.

En estas dos metodologías, al igual que ECU@Risk, se propone que todos y cada uno de los miembros a que sean partícipes del proceso de identificación de riesgos de seguridad y que puedan dar, como resultado, indicadores que permitan valorar la posible probabilidad de riesgo de una manera cualitativa, es decir, alta, media y/o baja, a la que finalmente se le deberá hacer un adecuado seguimiento.

Todas las metodologías sugieren utilizar escalas de riesgos, las mismas que involucran activos tangibles e intangibles, los mismos tienen un valor específico que está dado por un rango y una clasificación determinada. El primero hace referencia al daño o afección que pueden sufrir tanto los equipos como la información, posteriormente el segundo trata la probabilidad de que ocurra y a los efectos que causan los riesgos para organización.

Octave solo incluye una exploración limitada de la infraestructura informática. (Vásquez & López, 2016) acotan que "*las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad*". Esto en la vida real es totalmente válido, debido a que, quienes se convierten en custodios de información son los dueños de las plataformas informáticas, como sistemas contables, bases de datos de clientes, entre otros;

incrementando notablemente el factor riesgo sobre exposición, hurto o alteración de información por parte de un tercero a la organización.

Indistintamente de su autor o marca comercial, cada una de las metodologías mencionadas anteriormente están basadas en las normas ISO, normas que apoyan en la gestión de seguridad de la información y el tratamiento del riesgo. Toma, de cada una de ellas, los aspectos más relevantes en cada uno de los procesos que conforma un sistema de gestión de seguridad de la información SGSI; considerando a estos como la identificación y valoración de los activos de información, la identificación y valoración de vulnerabilidades y amenazas, el cálculo de riesgo y el establecimiento de alternativas de mitigación o contramedidas.

Magerit V3, la metodología gratuita española, es la más completa, ya que implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Según la guía Magerit, el análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, elementos que permiten controlar todas y cada una de las actividades involucradas con el manejo de información. La fase de tratamiento de riesgos organiza las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis, que concluyen en cuatro etapas cíclicas: Planificación, implementación y operación, monitorización y evaluación, y mantenimiento y mejora.

Toda metodología sugiere partir de la concienciación sobre los riesgos de información en la institución; una vez alcanzado este objetivo se podrán desarrollar políticas corporativas de fácil interpretación, las que aclararán obviamente el uso correcto e incorrecto de cada uno de los activos de información. Se podrían utilizar, como elementos informativos, las carteleras, la Intranet, así como la capacitación continua a todos los niveles, recordando

cuidados rutinarios y actividades especializadas, que inciden en la responsabilidad de cada uno de los involucrados.

Risk, Octave-S y Magerit son metodologías que están al alcance de cualquier organización de forma gratuita, acotando que la última versión de Risk fue en el año 2006, y la última actualización de Magerit en el 2013. Por su simplicidad, cualquiera de estas metodologías podría ser adoptadas por las organizaciones, empresas e instituciones del sector MPYME, considerando obviamente que han sido escritas para diferentes tipos de entorno político y socio económico.

La retroalimentación de cada una de las metodologías estudiadas ha permitido asimilar las mejores cualidades y características de cada una, en las que se ha podido comprobar que la gestión de riesgos se resume en la identificación y valoración de los activos de información, la identificación y valoración de amenazas, el cálculo de riesgos, la identificación de contramedidas y el manejo del riesgo residual; recalcando que cada una de ellas adopta las mejores prácticas de las ISO 27001, 27002, 27005 y 31000; utilizadas para la gestión de la seguridad de la información y la gestión del riesgo.

Las normas ISO influyen directamente en cada una de las etapas que contemplan las metodologías estudiadas. Las ISO 27001 y 27002 comprenden las mejores prácticas para establecer un ciclo de gestión de seguridad de la información, mientras que el aporte indiscutible sobre la gestión de riesgos está dado por las normas ISO 27005 e ISO 31000.

Al igual que las metodologías evaluadas, ECU@Risk comprende cuatro etapas clave:

La primera etapa comprende todo lo relacionado con los activos de información, esto es, actividades de identificación de activos de información y su valoración cualitativa, en la que se recomiendan al menos tres criterios para este propósito: Confidencialidad, Disponibilidad e Integridad. Magerit incluso sugiere considerar además de estos tres criterios, la Autenticidad para garantizar que el acceso al activo de información se da por un

usuario o sistema auténtico; y la Trazabilidad para rastrear las pistas dejadas por el sistema o persona que mantuvieron acceso a un activo de información.

En la segunda etapa se considera el análisis de amenazas. Aquí cada metodología plantea alternativas de identificación de amenazas físicas o de entorno, y las lógicas que podrían afectar a la disponibilidad, confidencialidad o integridad de la información organizacional. De cada una de las metodologías estudiadas, se puede rescatar que cada una de ellas utiliza criterios de valoración cualitativas, en algunos casos en tres niveles (alto, medio, bajo), o, en el caso de Magerit, una escala en 10 niveles, desde irrelevante hasta muy importante.

La tercera etapa consiste en calcular el riesgo basado en el impacto que podría ocasionar la materialización de una amenaza sobre la vulnerabilidad que presenta un activo de información. Cada metodología, incluyendo ECU@Risk, adopta las prácticas de las ISO 27005 e ISO 31000 para realizar tal tarea. Una vez que cierra esta etapa, procede con la siguiente.

La cuarta etapa consiste en aplicar mecanismos de mitigación de riesgos, conocidos también como salvaguardas o contramedidas. Estas, deben ser muy objetivas, realizables, alcanzables y, sobre todo, estar alineadas a los requerimientos organizacionales, acotando que dependen mucho de la valoración de los activos de información recibida en la primera etapa.

El ciclo se cierra con el cálculo del riesgo residual, es decir, una vez que se han identificado las contramedidas, se calcula el impacto del riesgo contra su mitigación. Por ejemplo, si la contramedida ante una amenaza de software ilegal, fue la adquisición de licencias; el riesgo residual se presentaría si el sistema operativo permite instalaciones de software por parte de los usuarios comunes de la red de datos. Así queda todavía la probabilidad de que la organización sea sancionada por uso ilegal de software.

Toda metodología debe estar alineada a la normativa vigente, por lo tanto, también se ha considerado el análisis de los aspectos legales, partiendo del estudio de la normativa internacional para luego compararla con las leyes ecuatorianas, en las que se ha podido ver, de manera inicial, un bajo nivel de madurez en estas últimas. Las acciones que ECU@Risk considera en sus procesos son legales, pues se encuentran dentro del marco normativo

vigente y no a la voluntad de cada persona, tema que fue discutido por (Jaramillo Palacios, 2014). Jaramillo menciona que el objeto de la Ley consiste en garantizar los derechos Constitucionales que hacen referencia al Derecho a la privacidad y el Derecho a la protección de datos personales. La Ley defiende los siguientes principios:

Legalidad, que hace referencia a la condición o acto realizado dentro del marco normativo, o sea, que debe realizarse de acuerdo a la Ley vigente y su jurisdicción, y no a la voluntad de las personas; Finalidad debido a que contribuye al logro del bien común de las personas que forman parte de una sociedad; y Libertad, debido a que la Ley implica en reconocer en cada persona su igualdad en el derecho a la libertad. Al formar parte de una sociedad independiente, algunas limitaciones a la libertad son esenciales para evitar otras restricciones de mayor incidencia (Merma Aroni, 2002).

La Calidad de los textos normativos, ya que las Leyes deben estar correctamente conformadas, deben ser claras y no ser anticonstitucionales. La Constitución de la República de Colombia menciona que el principio de Calidad consiste en que *"toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad."* (Presidencia de Colombia, 2014)

Consentimiento: en los casos en los que se requiere la anuencia de una persona para el tratamiento de sus datos personales; esto significa elegir el nivel de protección que cada persona quiere dar a la información a ella referida.

Transparencia: La Presidencia de Colombia menciona que Transparencia como el *"Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo*

el cumplimiento de los requisitos establecidos en esta ley" (Presidencia de Colombia, 2014).

Acceso y circulación restringida, hace referencia a que *"el derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de promover y generar una cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos fisicos y financieros".*

La información para cualquier institución o persona natural son muy importantes. Todas las metodologías estudiadas en los capítulos anteriores, se basan en función de un marco legal. Se puede agregar que Ecuador aún no tiene leyes claras en cuanto a la confidencialidad de la información, sin embargo, se sabe que son aspectos que deben ser considerados en una metodología, a manera de que esta sea un referente empresarial para la protección de información.

Para las MPYMES, ECU@Risk, dentro del marco legal organizacional, ha considerado los siguientes elementos:

- Procedimientos de concienciación a los usuarios y público en general
- Recolección constante de estadísticas y datos sobre incidentes informáticos (recopilación de los incidentes en bitácoras de control)
- Capacitación continua al personal implicado en la seguridad de la información.
- Actualización del marco normativo, es decir, del documento que contiene las políticas de seguridad de la información.
- Concienciación y compromiso de la gerencia, ya que la única forma de que un sistema de gestión de seguridad de la información funcione, es cuando se cuenta con el compromiso de respaldo de la alta dirección o la gerencia general.

Este marco legal es el que establece y regula las actividades que considera ECU@Risk como una metodología comprometida a mitigar el riesgo sobre los activos de información.

ECU@Risk cumple con la "calidad de los textos normativos" (Presidencia de Colombia, 2014), ya que incluye procedimientos claros que no van contra de la Constitución de la República del Ecuador. Este documento puede ser de interés público, y estar disponible en formatos accesibles para los solicitantes e interesados en él, obviamente considerando los derechos de propiedad intelectual.

Cada empresa, organización, negocio o institución debe estar consciente que la información que se genere en base a esta metodología es de carácter interno, y que no puede ser divulgada sin considerar los principios básicos de la seguridad de la información que han sido tratados en este documento: Confidencialidad, Integridad y Disponibilidad.

Ecuador aún no tiene leyes claras en cuanto a la confidencialidad de la información, sin embargo, han sido aspectos que fueron considerados en la formulación de esta metodología, la cual mantiene como objetivo el ser un referente empresarial para la protección de información.

Es vital que las MPYMES dentro de su marco legal organizacional considere crear conciencia a los usuarios y público en general; recolectar constantemente estadísticas y datos sobre incidentes informáticos, y registrarlos en bitácoras de control; establecer planes de capacitación continua al personal implicado en la seguridad de la información.

También es crucial que considere permanentemente la actualización del marco normativo que contiene las políticas de seguridad de la información; y la concienciación y compromiso de la gerencia, pues, como ya se había mencionado anteriormente, la única forma de que un sistema de gestión de seguridad de la información funcione, es cuando la alta dirección o la gerencia general respaldan los compromisos relacionados con el uso de los recursos de información.

ECU@Risk propone procesos para el inventario de activos de información, considerando como categorías principales las edificaciones o instalaciones, el hardware, el software, la información electrónica, la información en papel, la infraestructura de comunicaciones, los

medios de almacenamiento extraíbles y los recursos humanos; elementos con que toda organización del sector MPYME cuenta.

En la siguiente etapa, se han propuesto procesos y procedimientos para la identificación y valoración de riesgos y amenazas, los cuales incluyen matrices de apoyo para lograr tal objetivo. Estos riesgos luego serán tratados en la etapa de Tratamiento de riesgos, para lo cual se incluye una matriz de tratamiento, considerando una escala de 5 niveles de riesgo, partiendo desde el riesgo leve hasta alcanzar el riesgo extremo.

Dentro del tratamiento de riesgos se proponen aspectos que deberían considerarse en la elección de contramedidas, conociendo que estas deberán ser alcanzables, aplicables, aceptables, además de medibles y registrables.

Las políticas de seguridad resultantes de la aplicación de esta metodología, aportarán a las decisiones de gobierno que deben ser sancionadas en la empresa, y por esa razón, tal como lo establece ISACA en su metodología COBIT, son "*una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones)*".

Para que la metodología ECU@Risk se proyecte a COSO III, se han incluido aspectos relacionados con:

- La Identificación del contexto organizacional
- Evaluación de aspectos que conlleven a fraudes
- Identificación de actividades de control (Establecimiento de contramedidas)
- Actividades de monitoreo continuo y reporte a los interesados.

Considerando a COBIT 5, la perspectiva de la metodología a proponer se enfocaría a la gestión de riesgos, ya que se partiría de los procesos básicos de gobierno y gestión del riesgo, contemplando procedimientos para cada una de las fases involucradas: identificación, análisis, tratamiento, monitoreo y reporte permanente.

COBIT proporciona un cuadro de interacciones que se producen entre el Gobierno y la Gestión, las mismas que deberían ser consideradas en el análisis del contexto que formará parte de la metodología. Los procesos que incluya la misma, deberá considerar aspectos de gobierno y gestión, procesos de información (entradas, transformación y salidas), el análisis de las estructuras organizativas; principios, políticas y marcos de referencia organizacionales; cultura, ética y comportamiento (como valores compartidos); las personas y sus distintas habilidades; y los servicios, infraestructura y aplicaciones, que en conjunto conforman el sistema de información.

Finalmente, se puede acotar, que para su aplicación sea efectiva en una MPYME, será importante la participación de la gerencia en los procesos de gestión de riesgo, pues el compromiso que mantenga es primordial para lograr mitigar los riesgos en conjunto con un buen equipo de trabajo y de esta manera alcanzar las metas y objetivos corporativos que se fusionan en una visión empresarial.

Glosario

ABD: Administrador de Base de Datos.

Actitud ante el riesgo: Hace referencia al enfoque de una organización para evaluar y eventualmente perseguir, retener, tomar o apartar el riesgo.

Activo de información: Elemento que contiene información y que es fundamental para los procesos de negocio.

Apetito de riesgo: La cantidad y tipo de riesgo que una organización está dispuesta a obtener o conservar.

ASC: Área de Seguridad en Cómputo del (Áreas de seguridad en: Informática, Telemática). Se encarga de definir esquemas y políticas de seguridad en materia de cómputo para la entidad.

ATI: Administrador de Tecnologías de Información (Telemática). Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telemática de la Entidad.

BD: Base de datos.

CAV: Central Antivirus.

Centro de Cómputo: Cualquier oficina que cuenten con equipamiento de cómputo.

Centro de Operaciones de la Red: Es el área que se encarga del funcionamiento y operación de las Tecnologías de Información y comunicaciones (Telemática) en la organización

Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

Recurso informático: Cualquier componente físico o lógico de un sistema de información.

Red: Equipos de cómputo, sistemas de información y redes de telemática organizacional

SII: Sistema Integral de Información

Site: Espacio designado en la entidad a los equipos de telecomunicaciones y servidores.

Solución Antivirus: Recurso informático empleado en la organización para solucionar problemas causados por virus informáticos.

Telemática: Conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática ofreciendo posibilidades de comunicación e información.

TI: (Tecnologías de Información), conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de la Información (Antes conocido como TICs)

TIC: (Tecnologías de Información y Comunicaciones), ahora conocido como TI.

Tolerancia al riesgo: Una disposición de las partes interesadas o de la organización para asumir el riesgo después del tratamiento del mismo con el fin de lograr sus objetivos.

Treta: Amenaza que podría incidir sobre una vulnerabilidad.

Usuario: Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por la organización tales como equipos de cómputo, sistemas de información, redes de telemática.

Virus informático: Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

Vulnerabilidad: Punto débil de un activo de información.

Bibliografía y fuentes de consulta.

- ISACA, www.isaca.org, fecha de última consulta: 18 de noviembre de 2015.
- G Stoneburner, A Goguen, A Feringa, Risk management guide for information technology systems, 2002.
- Consejo Superior de Administración Electrónica, Magerit V3, www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/, Fecha de última consulta: 18 de noviembre de 2015.
- Microsoft, The Microsoft Risk Management Guide, 2006, http://www.microsoft.com/en-us/download/details.aspx?id=6232, Fecha de última consulta: 18 de noviembre de 2015.
- CERT, Software Engineering Institute, Carneige Mellon University, Octave Risk Analisys Methodology, http://www.cert.org/resilience/products-services/octave/, Fecha de última consulta: 18 de noviembre de 2015.
- Gobernanza de Internet en Ecuador, http://gobernanza.net.ec/infraestructura-y-estandarizacion/ciberseguridad/, Fecha de última consulta: 18 de noviembre de 2015.
- Ministerio de Tecnologías de información y comunicaciones de Colombia – MINTIC, http://www.mintic.gov.co/portal/604/w3-channel.html, Fecha de última consulta: 18 de noviembre de 2015.
- Instituto nacional de Ciberseguridad de España – INCIBE, https://www.incibe.es/que_es_incibe/, Fecha de última consulta: 18 de noviembre de 2015.
- Guía política pública de datos abiertos, Secretaria Nacional de la Administración Pública – SNAP, http://www.gobiernoelectronico.gob.ec/GPP-DA-v01-20141128-SNAP-SGE.pdf, Fecha de última consulta: 18 de noviembre de 2015.
- Plan Nacional de Gobierno Electrónico, http://www.gobiernoelectronico.gob.ec/, Fecha de última consulta: 18 de noviembre de 2015.
- Ley del Sistema Nacional de Datos públicos, Secretaría Nacional de Telecomunicaciones,http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf, Fecha de última consulta: 18 de noviembre de 2015.

Referencias

27001 Academy. (2015). *27001 academy*. Obtenido de http://www.iso27001standard.com/es/que-es-iso-27001/

Alcides, G. (2009). *Seguridad informática.* Antioquía, Colombia: Universidad de Antioquía.

AUDITOOL. (05 de 2013). *MODELO COSO III - MARCO INTEGRADO DE CONTROL INTERNO*. Recuperado el 18 de 01 de 2016, de http://www.cicinacional.com/images/Articulos/Guia_Marco_Integrado_de_Control_Interno_COSO_III.pdf

Azanza, B., & Bermeo, I. (2016). Manual de procedimientos para la gestión del proceso de Servucción dentro de la industria ecuatoriana de restauración; modelo de propuesta para "Parrilladas El Fogón". *Manual de procedimientos para la gestión del proceso de Servucción dentro de la industria ecuatoriana de restauración; modelo de propuesta para "Parrilladas El Fogón".* Unicersidad del Azuay, Cuenca.

Barrera, M. (2014). *Situación y desempeño de PYMES en el mercado internacional.* Quito: Camara de la Pequeña Industria del Pichincha.

Bernal, C. A. (2006). *Metodología de la Investigación.* México: Pearson Prentice Hall.

Borghello, C. (2009). *Seguridad de la Información - Segu.Info.* Obtenido de Legislación y Delitos Informáticos: http://www.segu-info.com.ar/delitos/delitos.htm

Burgos Salazar, J., & Campos, P. G. (2008). Modelo Para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío.

Cano, J. (2009). *Computación Forense: Descubriendo los rastros informáticos.* México: Alfaomega.

Castaño, P. (7 de Septiembre de 2014). *Metodología de Análisis de Riesgos: MAGERIT.* Obtenido de GR2DEST: http://blacksecurity.net/Gr2Dest/metodologia-de-analisis-de-riesgos-magerit/

Cavoukian, A. (2013). *SURVEILLANCE, THEN AND NOW, Securing Privacy in Public Spaces.* Ontario: Information and Privacy Commissioner.

Cocho, J. M. (Junio de 2006). MAGERIT Y LA NORMALIZACIÓN DE OTROS MODELOS. Sevilla, España.

Cordero Torres, G. (01 de 07 de 2015). Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información. Cuenca, Azuay, Ecuador.

Cordero, G. (2015). Estudio comparativo de las tecnologías MAGERIT y CRAMM, utilizadas para análisis y gestión de de riesgos de seguridad de la información. Cuenca, Azuay, Ecuador.

Cornell University Law School. (08 de 04 de 2016). *Legal Information Institute*. Obtenido de Fourth Amendment: https://www.law.cornell.edu/constitution/fourth_amendment

Crespo, E., & Cordero, G. (2016). Estudio comparativo de las tecnologías MAGERIT y CRAMM, utilizadas para análisis y gestión de de riesgos de seguridad de la información. *Utopía*, 24-27.

Garcés, H. (2000). *Investigación Científica.* Quito: Abya-Yala.

García Falconí, J. (07 de 02 de 2011). *Revista judicial*. Obtenido de derechoecuador.com: http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2011/02/07/la-proteccion-de-datos-personales

Gómez Vieites, Á. (2011). *Enciclopedia de la Seguridad Infomática.* México: AlfaOmega.

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid: ISACA® Framework. doi:978-1-60420-282-3

Jaramillo Palacios, F. (28 de 01 de 2014). *La protección de los datos personales en el Ecuador*. Obtenido de http://www.infodf.org.mx/dp/doctos/14/presenta/dia28/ecuador_fabian_jaramillo.pdf

Lima, M. d. (1984). Delitos electrónicos. *Criminalia*.

Merma Aroni, N. (2002). La Ley, fundamento de la sociedad o restricción de la libertad? *La Pluma del Conocimiento, 2, Bahá´í Library Online*.

Microsoft. (15 de Octubre de 2006). Obtenido de Microsoft: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx

Microsoft, C. (2006). *microsoft*. Obtenido de microsoft: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx

Minchala, P. (2016). *Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI.* Universidad del Azuay, Cuenca, Ecuador.

Ministerio de Hacienda y Administraciones Públicas de España. (Octubre de 2012). Magerit 3. Madrid, España.

Moncayo Racines, D. E. (1 de Agosto de 2014). Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/8499/1/CD-5741.pdf

Muñoz, D. C. (24 de Febrero de 2012). *dspace.* Obtenido de space: http://dspace.ups.edu.ec/bitstream/123456789/1442/5/Capitulo%202.pdf

Ochoa, C. (12 de 06 de 2015). *Netquest.* Obtenido de Muestreo No probabilistico: Muestreo por cuotas: http://www.netquest.com/blog/es/muestreo-por-cuotas/

Páez Rivadeneira, J. J. (13 de 01 de 2010). *Derecho Ecuador*. Obtenido de Protección de datos: http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2009/11/24/proteccion-de-datos

Pérez, M. (14 de 03 de 2011). *Administración de las operaciones en las PYME.* Obtenido de Observatorio PYME de la Universidad Andina Simón Bolivar: http://portal.uasb.edu.ec/UserFiles/381/File/MARCELA_PEREZ_2.pdf

Presidencia de Colombia. (6 de 03 de 2014). *Mas información mas derechos*. Obtenido de Ley 1712 de 2014 "Ley de Transparencia": http://masinformacionmasderechos.co/ley-1712-de-2014-ley-de-transparencia

Ritegno, E. O. (2012). *Gestión de Riesgos de TI.* Buenos Aires: Banco de la Nación Argentina.

Royer, J.-M. (2004). *Seguridad en la Informática de Empresa: riesgos, amenazas, prevención y soluciones.* Barcelona: Eni ediciones.

Superintendencia de Bancos y Seguros. (2012). Resolución JB-2012-2148. Quito, Pichincha, Ecuador.

Ulloa, S. J. (Febrero de 2015). *uta*. Obtenido de uta: http://repositorio.uta.edu.ec/bitstream/123456789/8654/1/Tesis_t975si.pdf

Universidad Andina Simón Bolivar. (2011). *Observatorio de la Pequeña y Mediana Empresa de la Universidad Andina Simón Bolivar.* Obtenido de http://portal.uasb.edu.ec/UserFiles/381/File/CENEC_NACIONAL.pdf

University of Adelaide. (2015). *The Risk Management Handbook.* Sydney: Legal and risk.

Vásquez, S., & López, D. (14 de 03 de 2016). Estudio comparativo entre las metodologías Microsoft Secure Risk Management y Octave. Cuenca, Azuay, Ecuador.

Yazar, Z. (2002). A qualitative risk analysis and management tool – CRAMM. *Information Security Reading Room.*, 6. SANS Institute.